KVM IP-BOX

IP - 101

User Manual

2009.05.11

Certifications

FCC

This equipment has been tested and found to comply with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:

(1) This device may not cause harmful interference
(2) This device must accept any interference received, including interference that may cause undesired operation.

CE

This equipment is in compliance with the requirements of the following regulations:
EN 55022: CLASS B

RoHS

All contents of this package, including products, packing materials and documentation comply with RoHS.

Contents

1. Product Overview 8
1.1 Introduction 8
1.2 Main Feature 8
2. Installation and Start up 9
2.1 Package Check List 9
2.2 Panel Views 9
2.3 System requirement 9
Hardware 9
Software 10
2.4 When the server is up and running 10
2.5 When the server is dead 10
2.6 Rack Mounting 10
2.7 Cable Connections (stand-alone) 11
2.8 Cable Connections (with Multi-port KVM Switch) 12
2.9 LED Indicators, Button 14
3. Configuration 15
3.1 Initial IP Configuration via Network 15
3.2 Configuration Setup via Serial Console 18
3.3 Keyboard, Mouse, and Video configuration 19
3.3.1 IP-101 keyboard settings 19
3.3.2 Remote Mouse Settings 19
3.3.3 Automatic mouse speed and mouse synchronization 19
3.3.4 Host system mouse settings 20
3.3.5 Single and Double Mouse Mode 20
3.3.6 Recommended Mouse Settings 21
3.3.7 Video Modes 21
4. Usage 22
4.1 Prerequisites 22
4.2 Login into the IP-101 and logout 23
4.2.1 Login into the IP-101 23
4.2.2 Login out from the IP-101 25
4.3 The Remote Console 26
4.3.1 Main Window of Remote Console 26
4.3.2 Control Bar of Remote Console 27
4.3.3 Status Line of Remote Console 37
5. Menu Options 38
5.1 Remote Control 38

5.1.1 KVM Console 39
5.1.2 Telnet Console 39
5.2 Virtual Media 41
5.2.1 Floppy Disk 42
5.2.2 CD–ROM Image 44
5.2.3 Drive redirection 48
5.2.3.1 Driver Redirection Utility Installation 51
5.2.3.2 Built-in Java Drive Redirection 55
5.2.4 Options 57
5.2.4.1 Creating an Image 57
5.2.4.1.1 Floppy Images 57
5.2.4.1.2 CD ROM/ISO Images 58
5.3 User Management 60
5.3.1 Change Password 60
5.3.2 Users and Groups 61
5.4 KVM Settings 62
5.4.1 User Console 63
5.4.2 Keyboard/Mouse 67
5.4.3 Video 69
5.5 Device Settings 70
5.5.1 Network 70
5.5.2 Dynamic DNS 73
5.5.3 Security 76
5.5.4 Certificate 79
5.5.5 Serial Port 82
5.5.6 Date / Time 84
5.5.7 Event Log 85
5.6 Maintenance 88
5.6.1 Device Information 88
5.6.2 Even log 89
5.6.3 Update Firmware 90
5.6.4 Unit Reset 91
6. Technical Specifications 92
7. Troubleshooting 93
8. FAQs 95
9. Addendum 97
A. Key Codes 97
B. Video Modes 98
C. User Role Permissions 98
D. IP-101 TCP port number 99

E. Bandwidth Consumption 100
F. Cable Connectors 101
G. Well-Known TCP/UDP Port Numbers 102
H. Protocol Glossary 103

Figures

Figure 2-1 Panel Views 9
Figure 2-2 Cable Connections (stand-alone) 11
Figure 2-3 Cable Connections (with a Multi-port KVM Switch) 13
Figure 4-1 The Internet Explorer displaying the encryption key length 23
Figure 4-2 Remote Console Control Bar 27
Figure 4-3 Remote Console Options Menu 28
Figure 4-4 Remote Console Exclusive Mode 29
Figure 4-5 Remote Console Options Menu:Scaling 29
Figure 4-6 Remote Console Options Menu:Cursor 31
Figure 4-7 Video Settings Panel 32
Figure 4-8 Soft Keyboard 33
Figure 4-9 Soft Keyboard Mapping 33
Figure 4-10 Remote Console Confirmation Dialog 34
Figure 4-11 Encoding Compression 35
Figure 4-12 Predefined Compression 35
Figure 4-13 Lossy Compression 36
Figure 4-12 Encoding Color depth 36
Figure 4-13 Status line 37
Figure 4-14 Status line transfer rate 37
Figure 5-1 KVM Console 39
Figure 5-2 Telnet Console 39
Figure 5-3 Virtual Media - Floppy Disk 42
Figure 5-4 Virtual Media – CD-ROM Image 45
Figure 5-5 Explorer context menu 47
Figure 5-6 Share configuration dialog 48
Figure 5-7 Options of Drive Redirection 49
Figure 5-8 Drive Redirection Setup 51
Figure 5-9 Drive Redirection dialog 52
Figure 5-10 Built-in Java Drive Redirection 55
Figure 5-11 USB mass storage option 57
Figure 5-12 RawWrite for Windows selection dialog 58
Figure 5-13 Nero selection dialog 59
Figure 5-14 Setting Password 60
Figure 5-15 User Console Setting 64
Figure 5-16 Keyboard and Mouse Settings 67
Figure 5-17 Video Settings 69
Figure 5-18 Network Settings 71

Figure 5-19 Dynsmic DNS 73
Figure 5-20 Dynamic DNS Scenario 74
Figure 5-21 Device Security 76
Figure 5-22 Chain Rules of IP Filtering 77
Figure 5-23 Certificate Settings 79
Figure 5-24 SSL Certificate Upload 80
Figure 5-25 CSR string 80
Figure 5-26 Serial Port 82
Figure 5-27 Date / Time 84
Figure 5-28 Event Log 85
Figure 5-29 Device Information 88
Figure 5-30 Connected Users 89
Figure 5-31 Event Log List 89
Figure 5-32 Update Firmware 90
Figure 5-33 Unit Reset 91

1. Product Overview

1.1 Introduction

The KVM IP-BOX (hereafter call IP-101 for simplicity) redirects local keyboard, mouse and video data to a remote administration console. It allows you to control one or many computers locally at the server site or remotely via the Internet using a standard browser. You can securely gain BIOS level access to systems for maintenance, support, or failure recovery over the Internet. Communication is secure via SSL authentication and encryption. Use in conjunction with a KVM switch for multiple-server access.

The IP-101 provides convenient, remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video signal and transmits it with keyboard and mouse signals to and from a remote computer. IP-101 provides a non-intrusive solution for remote access and control. Remote access and control software runs on its embedded processors only but not on mission-critical servers, so that there is no interference with server operation or impact on network performance.

1.2 Main Feature

- Manage servers around the world.
- Rack mountable
- KVM (keyboard, video, and mouse) access over IP or analogous telephone line (modem needed).
- Full control under any OS, in BIOS mode, during boot, at Blue Screens
- No additional software necessary on servers
- SSL Certificate management
- 256-bit SSL encryption of all transmitted data
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization
- Automatic adjustment of data rate to transmission line
- Remote mass storage control and redirection
- Can be remote controlled over java-enabled Browsers
- Firmware update via web interface
- Port to connect a user console for direct analogous access to KVM switch
- Can be used with most standard KVM

2. Installation and Start up

2.1 Package Check List

The IP-101 package consists of followings items:

1x The single port IP-101 unit
1x Quick Start Guide
1x CD-ROM (software utilities and User's manual)
1x Power Adapter (DC 12V / 1.25A)
1x 1.2M RS-232 cable
1x 1.2M USB A-to-Mini cable
1x 1.2M 3-in-1 KVM cable
1x Rack Mount Kit (Brackets and screws)

2.2 Panel Views

<Font View>

<Back View>

Figure 2-1 Panel Views

2.3 System requirement

Hardware

Item Description	
Local host side	One PC or Server or the console port of KVM switch
Local console side	One PS/2 Keyboard, one PS/2 Mouse and one monitor
Remote Console side	One PC or Multiple PCs are linked into the network

Software

Item Description	
Local host side	No additional software necessary
Remote Console side	(1) Java Runtime Environment : version 1.4.2 or above (2) Browser: Microsoft Internet Explorer version 6.0 or above or Netscape or Mozilla or Safari

2.4 When the server is up and running

The IP-101 gives you a full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and to send special commands to the server. You can also perform periodic maintenance of the server. Using the Console Redirection Service, you are able to do the following:

I. Reboot the system
II. Watch the boot process.
III. Boot the system from a separate partition to load the diagnostic environment.
IV. Run special diagnostic programs

2.5 When the server is dead

Obviously, fixing hardware defects is not possible through a remote management device. Nevertheless IP-101 gives the administrator valuable information about the type of a hardware failure. Serious hardware failures can be categorized into five different categories with different chances to happen:

I. Hard disk failure 50%
II. Power cable detached, power supply failure 28%
III. CPU, Controller, main board failure 10%
IV. CPU fan failure 8%
V. RAM failure 4%

Using IP-101, administrators can determine which kind of serious hardware failure has occurred

Type of failure	Detected by
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply	Server remains in power off state after power on command has been given.
CPU Controller, main board failure.	Power supply is on, but there is no video output.
CPU fan failure	By server specific management software
RAM failure	Boot-Sequence on boot console

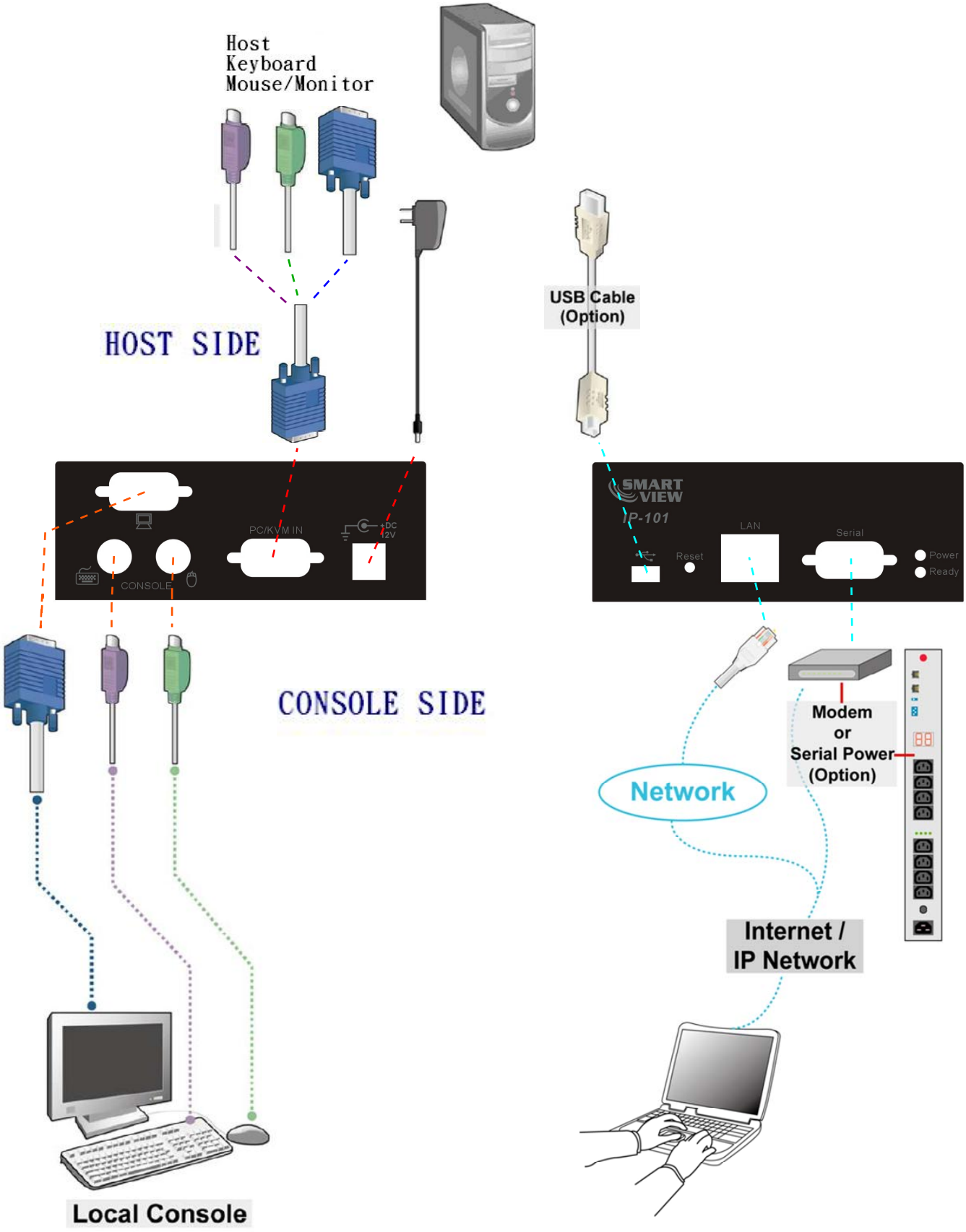
2.6 Rack Mounting

In addition to desk top placement, the IP-101 can be mounted on 19"/1U rack:

1. Screw the mounting brackets into the sides of the unit.
2. Slide the unit into the rack and secure it to the rack.

2.7 Cable Connections (stand-alone)

The figure below depicts the installation connection.



Connect cables to the Host and Console devices as the figure depicts above. Leave the Serial interface open for now. After applying power to the unit, it'd take about 60 seconds to complete the bootup process, and then enter normal running state.

Please perform the following steps:

1. Power down your computer and IP-101
2. Connect the power supply to IP-101
3. Connect the monitor to the IP-101 console side.
4. Connect the keyboard to the IP-101 console side.
5. Connect the mouse to the IP-101 console side.
6. Connect a VGA cable (HD-15 Male / Male) with the Male side to both of the host computer/KVM and the host port of the IP-101.
7. Connect one purple end of 3-in-1 cable to the PS/2 keyboard port on the host computer/KVM, and the other end of 3-in-1 cable to the host PS/2 mouse port on the IP-101.
8. Connect one green end of 3-in-1 cable to PS/2 mouse port on the host computer/KVM, and the other end of 3-in-1 cable to the host PS/2 keyboard port on the IP-101.
9. (Optional) Connect the type A connector of USB A-Mini cable to the host computer, while using remote mass storage control.
10. Connect Ethernet to LAN port and/or modem to serial port, depending on how you want to access to the IP-101.

2.8 Cable Connections (with Multi-port KVM Switch)

Instead of connecting to a computer, the IP-101 host side can be connected to a multi-port KVM Switch system. In installation procedures are as for stand alone computer, except that the host signals are connected to the Local Console of the KVM Switch. The figure below depicts the installation connection.

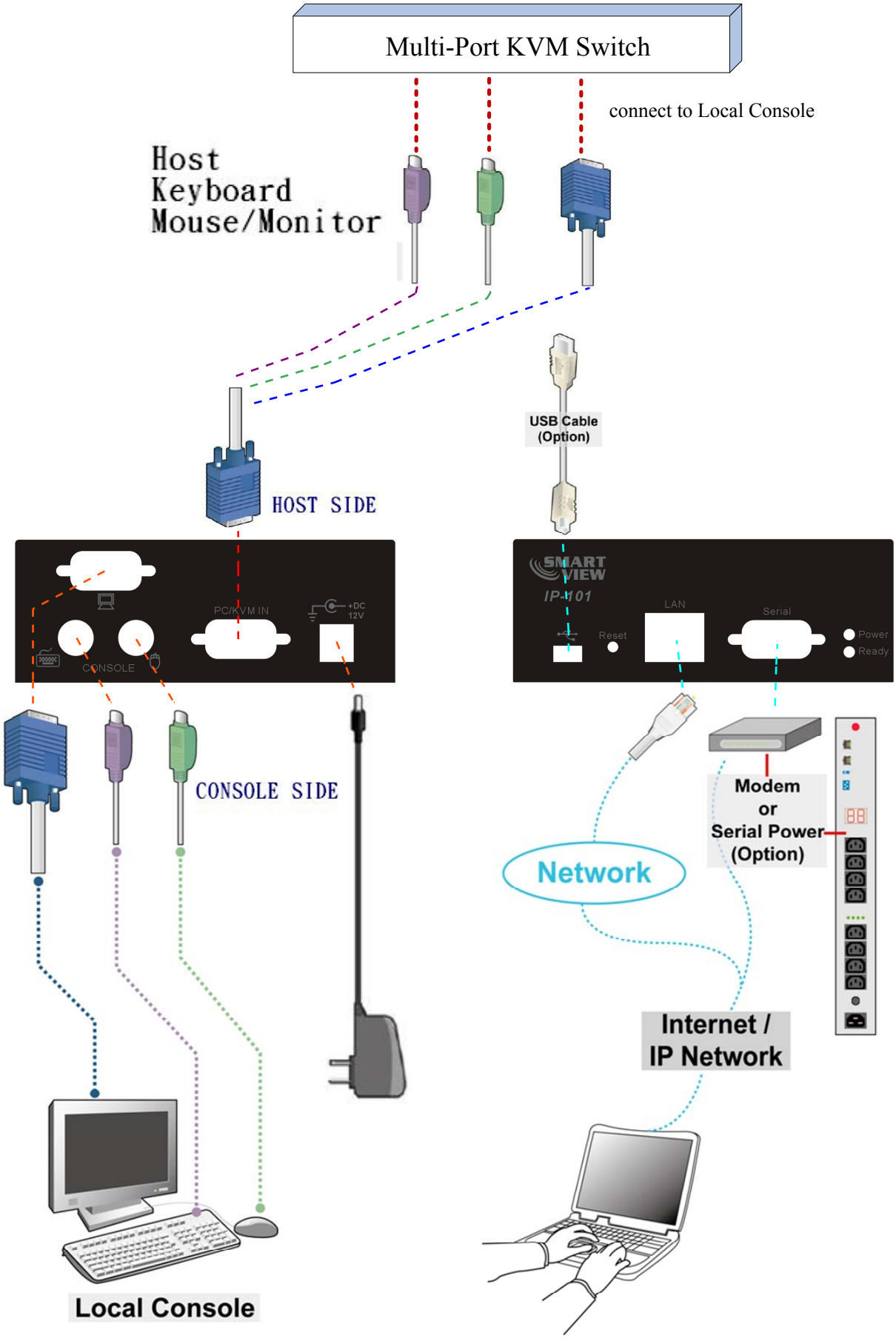


Figure 2-3 Cable Connections (with a Multi-port KVM Switch)

2.9 LED Indicators, Button

LED	Indication
Power	**GREEN** – on when power applied
	Ethernet Link/Act/10/100Mbps:
LAN	**Orange** -- Ethernet data in activity connection **Green** -- 100BaseT Ethernet connection established *Blinking:* *ON: when data in activity and link connected*
Link	RED -- blinking when data in activity

- **RESET** button: on the rear panel, press the button to reboot the IP-101 unit

3. Configuration

3.1 Initial IP Configuration via Network

The Factory default settings for the IP-101 unit are as below:

DHCP: Disable

Default IP address: 192.168.0.70

Default Net Mask: 255.255.255.0

If DHCP mode is enabled (IP auto configuration = DHCP), the IP-101 will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the IP-101. You can find the MAC address labeled on the bottom side of the metal housing.

There is a Network Setup Software tool **(PSetup)** for setting up the network configuration (IP address, Subnet mask, DHCP, etc). It is useful when you want to change the network settings or you can not access to the unit due to not knowing the network settings of the unit. In this case, you can view or change the settings via this utility.

IP-101 Setup Tool

If this initial configuration does not meet your local requirements, use the setup tool to change the configurations to your needs. The setup tool **PSetup** can be found on the CD ROM delivered with this package. You can follow the procedures described below.

DHCP

If you have installed the IP-101 on a network that enables DHCP, you can use the **PSetup** to find out the IP-101's IP.

(1) Plug Ethernet cable to IP-101. IP-101 will get an IP via DHCP.

(2) Using **PSetup** to look for IP-101.

a. Click **Refresh Devices** button to detect connected devices

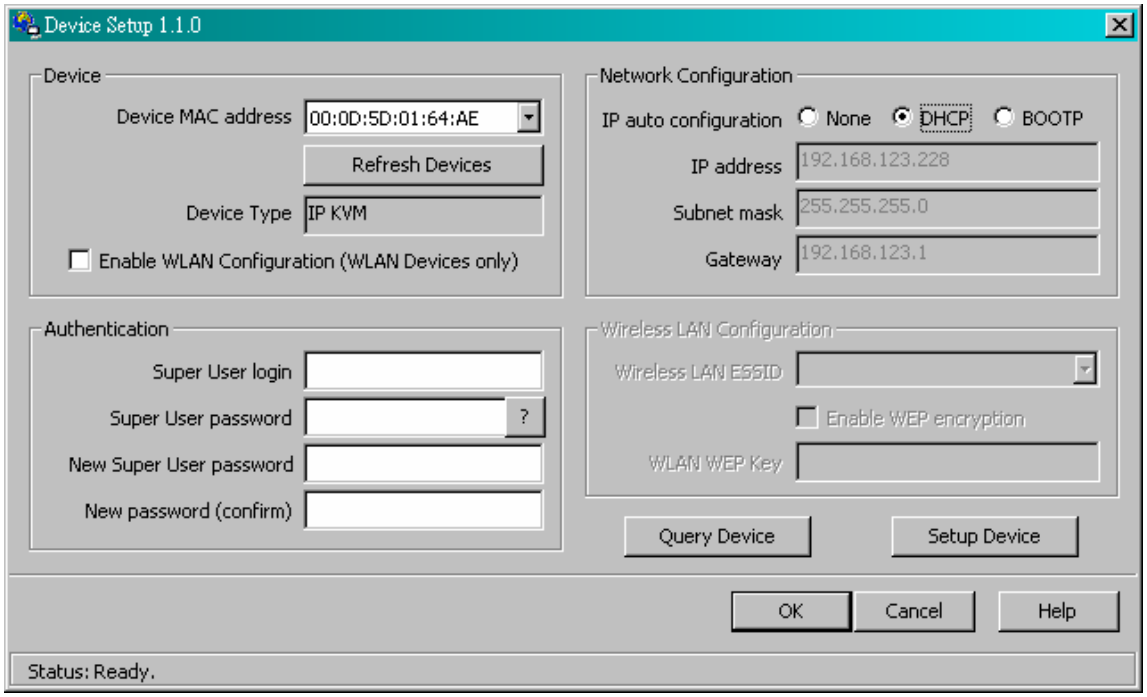
b. Select MAC address of the IP-101 in "Device MAC address" box. You can find the MAC address labeled on the bottom side of I-BOX. MAC address is detected as connection from computer and IP-101 is valid through USB or network.

c. If wireless connection is implemented, tick "Enable Wireless Connection..."

d. Click **Query Device** to find the IP configuration on the right pane.

Notes:

- **BOOTP**, a static configuration protocol, uses a table that maps IP addresses to physical addresses.
- **DHCP**, an extension to BOOTP that dynamically assigns configuration information. DHCP is backward compatible with BOOTP.

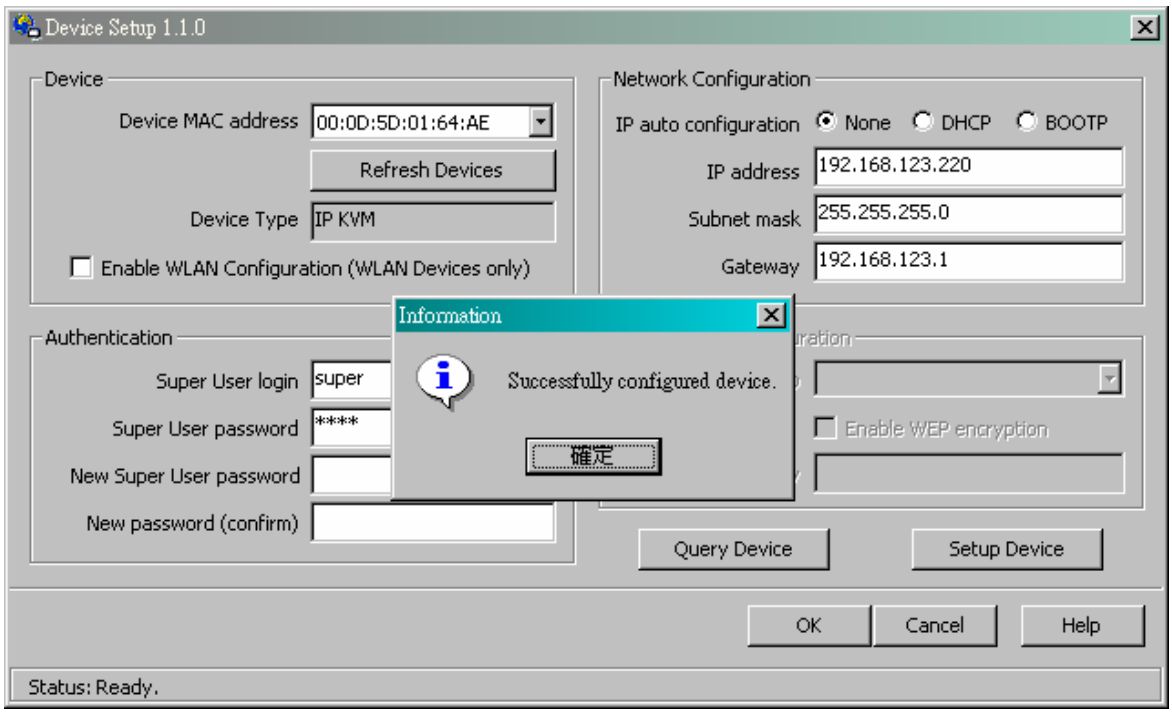


Setup fixed IP

a. Setup "IP auto configuration" as "**None**" ; setup IP address and Subnet mask

b. Enter Super user login and password for Authentication (default : super/pass)

c. Click **Setup Device**. If super login was authenticated, it'll show "Successfully configured device". Otherwise it'll show "Permission Denied".



Authentication

To adjust the authentication settings, enter your login as a super user, and change your password.

Super user login

Enter the login name of the super user. The initial value is “super”. All characters are in lower case.

Super user password

Enter the current password for the super user. This initial value is “pass”. All characters are in lower case.

New super user password

Enter the new password for the super user.

New password (confirm)

Re-type the new password for the super user for confirmation.

To close the window and accept the changes, press the “OK” button; otherwise press the “Cancel” button.

3.2 Configuration Setup via Serial Console

For using serial terminal, the IP-101 has a serial line interface (host side). This connector is compliant with the RS-232 serial line standard. The serial line has to be configured with the parameters given in Table below.

Parameter V	alue
Bits/second 1	15200
Data bits	8
Parity No	
Stop bits	1
Flow Control	None

When configuring with a serial terminal, e.g., Hyper Terminal, reset the IP-101 and immediately press the “ESC” key. You will see some device information, and a “=>” prompt. Enter “config”, press “Enter” key and wait for a few seconds for the configuration questions to appear.
As you proceed, the following questions will appear on the screen. To accept the default values shown in square brackets below, press “Enter” key.

IP auto configuration (none/dhcp/bootp):
IP [192.168.0.70]:
Net mask [255.255.255.0]:
Gateway (0.0.0.0 for none) [0.0.0.0]:

IP auto-configuration

With this option, you can specify whether the IP-101 should get its network settings from a DHCP or BOOTP server. For DHCP, enter “dhcp”, and for BOOTP enter “bootp”. If you do not specify any of these, the IP auto-configuration is disabled and subsequently you will be asked for the following network settings.

IP address

The IP address the IP-101. This option is only available if IP auto-configuration is disabled.

Net mask

The net mask of the connected IP subnet. This option is only available if IP auto-configuration is disabled.

Gateway address

The IP address of the default router for the connected IP subnet. If you do not have a default router, enter 0.0.0.0. This option is only available if IP auto-configuration is disabled.

3.3 Keyboard, Mouse, and Video configuration

Between the IP-101 and the host, there are two interfaces available for transmitting keyboard and mouse data: USB and PS/2. The correct operation of the remote mouse depends on several settings which will be discussed in the following subsections.

3.3.1 IP-101 keyboard settings

The IP-101 settings for the host's keyboard type have to be corrected in order to make the remote keyboard work properly. Check the settings in the IP-101 Web front-end. See section 6.5.2 for details.

3.3.2 Remote Mouse Settings

A common seen problem with KVM devices is the synchronization between the local and remote mouse cursors. The IP-101 addresses this situation with an intelligent synchronization algorithm. There are two mouse modes available on the IP-101:

Auto mouse speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.

Fixed mouse speed

This mode just translates the mouse movements from the Remote Console in a way that one pixel move will result in n-pixel moves on the remote system. This parameter n is adjustable with the scaling. Please note that this works only when mouse acceleration is turned off on the remote system.

3.3.3 Automatic mouse speed and mouse synchronization

The automatic mouse speed mode performs the speed detection during mouse synchronization. Whenever the local and remote mouse cursors move synchronously or not, there are two ways for re-synchronizing local and remote mouse cursors:

Fast Sync

The fast synchronization is used to correct a temporary, but fixed skew. Choose the option using the Remote Console options menu or press the mouse synchronization hotkey sequence in case you defined one.

Intelligent Sync

If the fast sync does not work or the mouse settings have been changed on the host system, use the intelligent resynchronization. This method takes more time than the fast one and can be accessed with the appropriate item in the Remote Console option menu. The intelligent synchronization requires a correctly adjusted picture. Use the auto

adjustment function to setup the picture, and make sure that there are no window at the top left corner of the remote desktop that are able to change the mouse cursor shape from the normal state. The Sync mouse button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a fast sync, except in situations where the KVM port or the video mode changed recently.

Note: At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

3.3.4 Host system mouse settings

The host's operating system knows various settings from the mouse driver.

> **Note**: The following limitations do not apply in case of USB and Mouse Type "Windows >= 2000, MacOSX".

While the IP-101 works with accelerated mice and is able to synchronize the local with the remote mouse pointer, there are the following limitations, which may prevent this synchronization from working properly:

Special Mouse Driver

There are mouse drivers that influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.

Windows XP Mouse Settings

Windows XP knows a setting named "improve mouse acceleration", which has to be deactivated.

Active Desktop

If the Active Desktop feature of Microsoft Windows is enabled do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

Navigate your mouse pointer into the upper left corner of the applet screen and move it slightly forth and back. Thus the mouse will be resynchronized. If re-synchronizing fails, disable the mouse acceleration and repeat the procedure.

3.3.5 Single and Double Mouse Mode

The information above applies to the Double Mouse Mode, where remote and local mouse pointers are visible and need to be synchronized. The IP-101 also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode

in the open Remote Console and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode, it is necessary to define a mouse hotkey in the Remote Console Settings Panel. Press this key to free the captured local mouse pointer.

3.3.6 Recommended Mouse Settings

For the different operating systems we can give the following advice:

MS Windows

In general, we recommend the usage of a mouse via USB. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option “enhance pointer precision” in the Control Panel. In general, we recommend the usage of a mouse via USB. Choose USB
without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP
disable the option enhance pointer precision in the Control Panel.

SUN Solaris

Adjust the mouse settings either via xset m 1 or use the CDE Control Panel to set the mouse to “1:1, no acceleration”. As an alternative you may also use the Single Mouse Mode.

MAC OS X

We recommend using the Single Mouse Mode.

3.3.7 Video Modes

The IP-101 recognizes a limited number of common video modes. When running X11 on the host system, please do not use any custom mode lines with special video modes. If you do, the IP-101 may not be able to detect them. We recommend using any of the standard VESA video modes, instead.

4. Usage

4.1 Prerequisites

The IP-101 features an embedded operating system and applications offering a variety of standardized interfaces. This chapter will describe both these interfaces, and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family, thus they can be accessed using the LAN port of the device.

The following interfaces are supported:

HTTP/HTTPS

Full access is provided by the embedded web server. The IP-101 environment can be entirely managed using a standard web browser. You can access the IP-101 using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

Telnet

A standard Telnet client can be used to access an arbitrary device connected to the IP-101's serial port via a terminal mode.

The primary interface of the IP-101 is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.

In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.4.2 or above. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your IP-101 using the administration forms displayed by the browser itself.

For secure connection to the IP-101, we recommend the following browsers versions:

- Microsoft Internet Explorer version 6.0 or higher
- Netscape Navigator 7.0 or Mozilla 1.6 or higher

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol. Strong security is only assured by using a key length of 128 Bit. Some of the old browsers do not have a strong 128 Bit encryption algorithm.

Using the Internet Explorer, open the menu entry “?” and “Info” to read about the key length that is currently activated. The dialog box contains a link that leads you to information on how to upgrade your browser to a state of the art encryption scheme. Figure below shows the dialog box presented by the Internet Explorer 6.0.

Figure 4-1 The Internet Explorer displaying the encryption key length

Newer web browsers generally support strong encryption on default.

4.2 Login into the IP-101 and logout

4.2.1 Login into the IP-101

Launch your web browser. Direct it to the address of your IP-101, which you configured during the installation process. The address used might be an IP address or a dom ain name, in the case where you have given your IP-101 a sy mbolic name in the DNS. For instance, type the following in the URL field of your browser when establishing an unsecured connection:

http://<IP address of IP-101>

When using a secure connection, type in:

https://<IP address of IP-101>

This will lead you to the IP-101 login page as shown below

The IP-101 has a built-in super user that has all permissions to administrate your IP-101:

Username	super (factory default)
Password	pass (factory default)

Warning

The user “super” is not allowed to login via the serial interface of the IP-101.

Warning

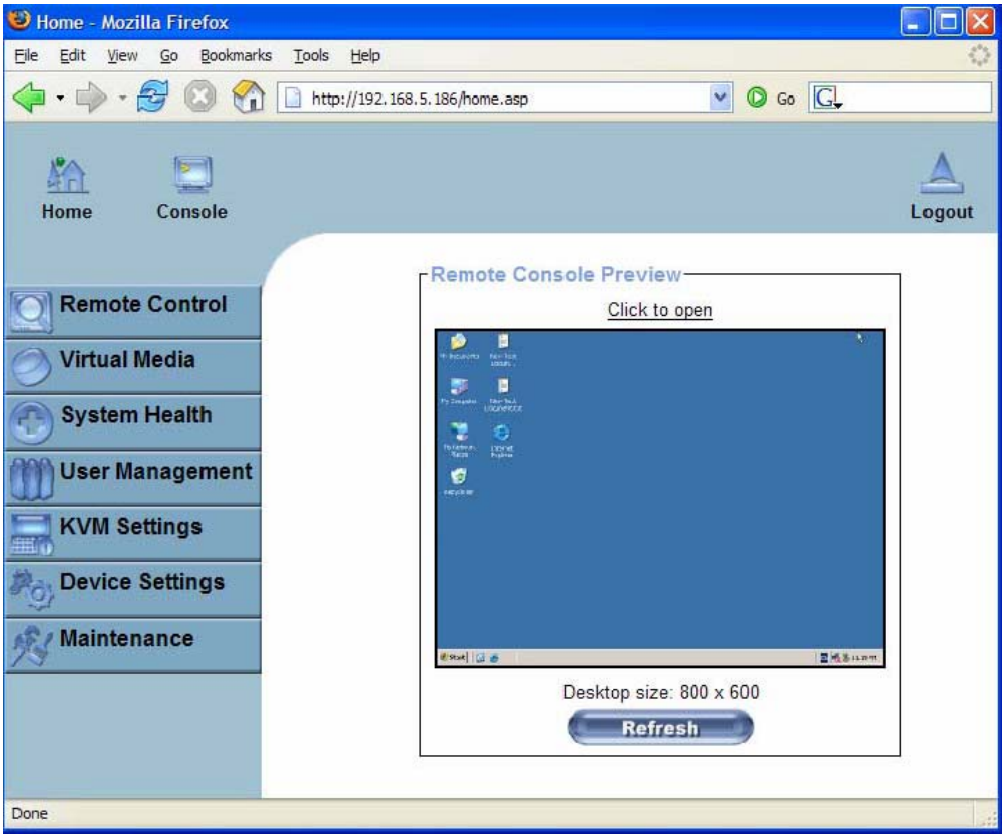
Please make sure to change the super user password immediately after you have installed and accessed your IP-101 for the first time. Unchanging of the password for the super user is a severe security risk and might result in unauthorized access to the IP-101 and to the host system including all possible consequences!

Warning

Your web browser has to accept cookies, or else login is not possible.

Navigation

Having logged into the IP-101 successfully, the main page of the IP-101 appears. This page consists of three parts; each of them contains specific information. The buttons on the upper side allow you to navigate within the front end. Within the right frame, task-specific information is displayed that depends on the section you have chosen before.



The Buttons of the front end:

Return to main page of IP-101 access page.

Open the IP-101 remote console.

Exit from the IP-101 front end.

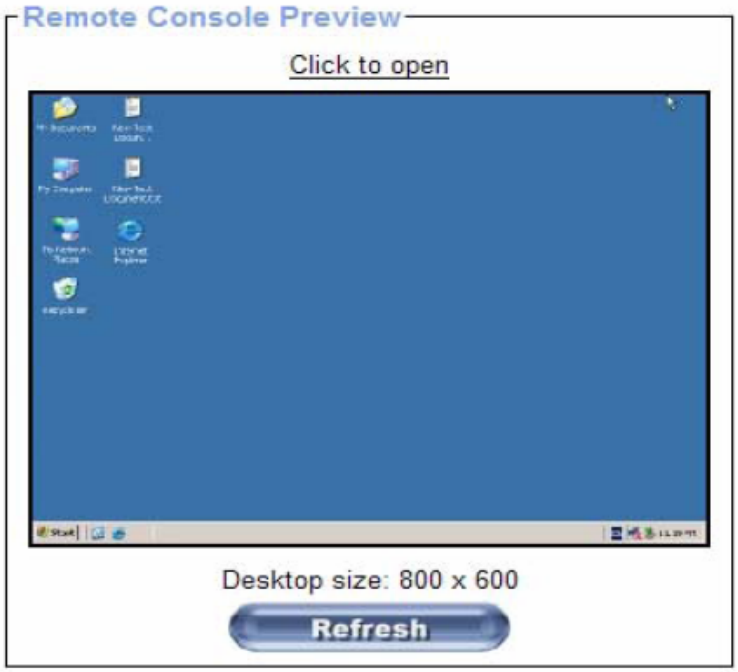
Warning

If there is no activity for 30 minutes, the IP-101 will log you out, automatically. A click on one of the links will bring you back to the login screen.

Remote Console Preview

Click on **Click to open** to start the remote console redirection.

Click on **Refresh** to refresh the picture.



4.2.2 Login out from the IP-101

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed in case there is no activity for 30 minutes.

4.3 The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that IP-101 controls.

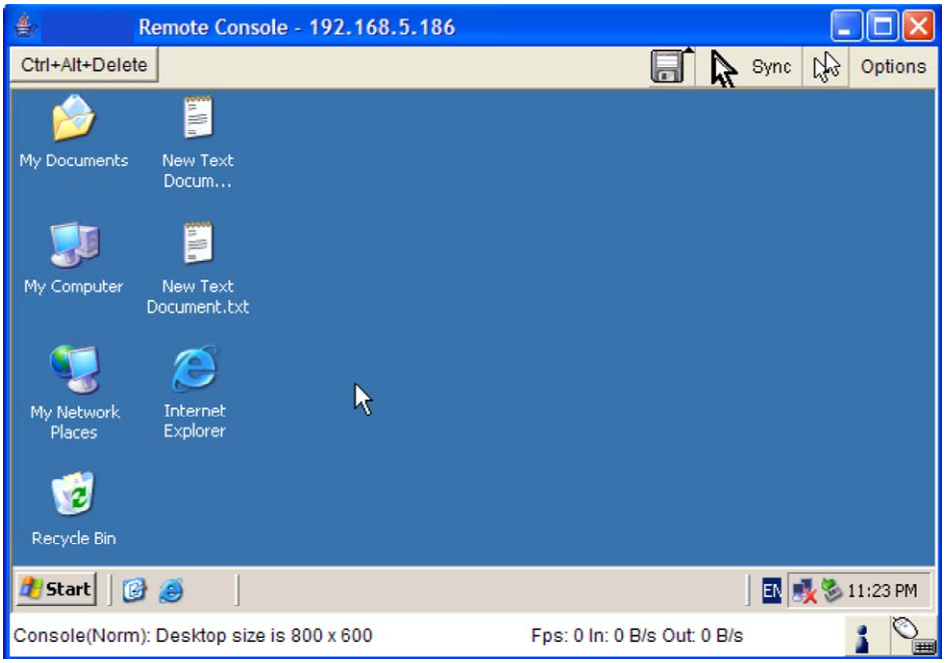
The Remote Console window is a Java Applet that tries to establish its own TCP connection to the IP-101. The protocol that is run over this connection is neither HTTP or HTTPS, but RFB (Remote Frame Buffer Protocol). As default, RFB tries to establish a connection to TCP port number 443. Your local network environment has to allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

In case the IP-101 is connected to your local network environment and your connection to the Internet is available using a proxy server only without NAT being configured, the Remote Console is very unlikely to be able to establish the desired connection. This is because today's web proxies are not capable of relaying the RFB protocol.

In case of problems, please consult your network administrator in order to provide an appropriate networking environment.

4.3.1 Main Window of Remote Console

To open the KVM console either click on the icon **Console** or **Remote Control > KVM Console** of the menu entry on the left or **Click to open** of the console picture on the right.



Starting the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly in the same way as if you were sitting locally in front of the screen of your remote system. That means keyboard and mouse

can be used in the usual way. However, be aware of the fact that the remote system will react to keyboard and mouse actions with a slight delay. The delay depends on the bandwidth of the link to which you use to connect to the IP-101.

With respect to the keyboard, the very exact remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the remote host system. If you use a German administration system, and your host system uses a US English keyboard layout, for instance, special keys on the German keyboard will not work as expected. Instead, the keys will result in their US English counterpart. You can circumvent such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

The Remote Console window always tries to show the remote screen with its optimal size. That means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window system as usual.

Warning

In difference to the remote host system, the Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus.

4.3.2 Control Bar of Remote Console

The upper part of the Remote Console window contains a control bar. Using its elements you can see the state of the Remote Console and adjust the local Remote Console settings. A description for each control follows.

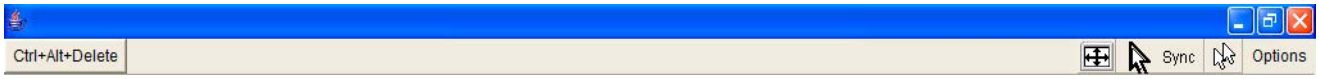
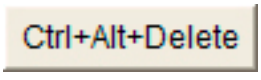


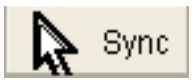
Figure 4-2 Remote Console Control Bar

Ctrl+Alt+ Delete 

Special button key to send the “Control Alt Delete” key combination to the remote system (see also section 6.4.1 for defining new button keys).

Auto Adjust button

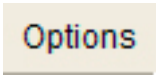
If the video display is of bad quality or distorted in some way, press this button and wait a few seconds while the IP-101 tries to detect the video mode of VGA port to the controlled host and adjust itself for the best possible video quality.

Sync mouse 

Activates the mouse synchronization process. Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on the host.

Single/Double mouse mode

Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.4.2 or higher.

Options 

To open the Options menu, click on the button “Options”.

Figure 4-3 Remote Console Options Menu

A short description of the options as follows.

- **Monitor Only**

  Toggles the Monitor only filter on or off. If the filter is switched on no remote console interaction is possible, and monitoring is possible.

- **Exclusive Access**

If a user has the appropriate permission, he or she can force the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access, or logs off.

A change in the access mode is also visible in the status line.

Figure 4-4 Remote Console Exclusive Mode

- **Scaling**

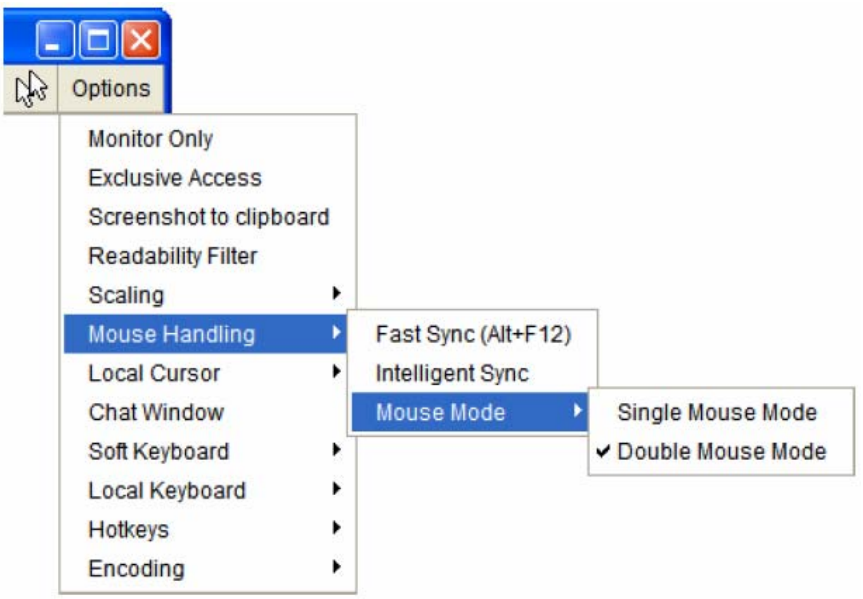
Allow you to scale down the Remote Console. You can still use both mouse and keyboard, however the scaling algorithm will not preserve all display details.

When you designate 25%, 50%, or100% scaling, the size of Remote Console window is calculated according to the remote host video setting with scaling algorithm execution. When you designate “Scale to fit”, the remote video displaying is scaled to fit the size of Remote Console window.

Figure 4-5 Remote Console Options Menu:Scaling

- **Mouse Handling**

The submenu for mouse handling offers two options for synchronizing the local and the remote mouse cursors.



Fast Sync --

The fast synchronization is used to correct a temporary, but fixed skew.

Intelligent Sync --

Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

Warning
This method takes more time than the fast one and requires a correctly adjusted picture. Use the auto adjustment function to setup the picture.

- **Local Cursor**

Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine; a version of 1.4.2 or above offers the full list.

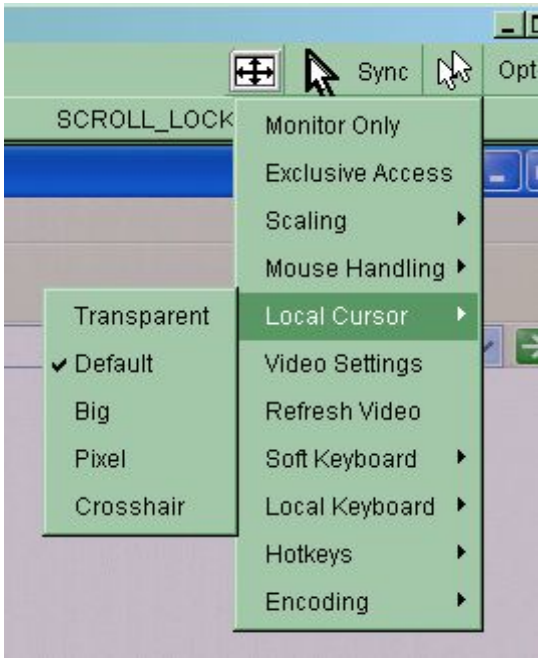


Figure 4-6 Remote Console Options Menu:Cursor

- **Video Settings**

Opens a panel for changing the IP-101 video settings. IP-101 features two different dialogs, which for adjusting the video settings.

Video Settings through the HTML-Frontend

To enable local video port, select this option. This option decides if the local video output of IP-101 is active and passing through the incoming signal from the host system.

The option Noise Filter defines how IP-101 reacts to small changes in the video input signal. Turning on the noise filter can help reduce video flickering that is often caused by distortions, as well as lowering unnecessary bandwidth consumption. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Video Settings through the remote console

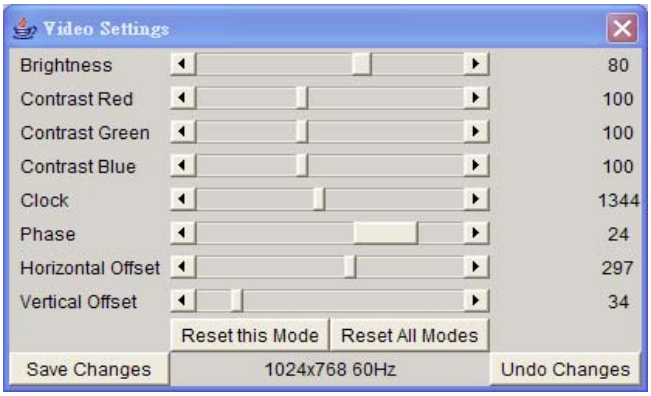


Figure 4-7 Video Settings Panel

Brightn ess Controls the brightness of the picture

Contrast Controls the contrast of the picture

Clock Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjuction with the auto adjustm ent procedure should be adequate for all common configurations. If the picture quality is still bad after auto adjustment you may try to change this setting together with the sampling phase to achieve a better quality.

Phase Defines the phase for video sam pling, used to control th e display quality together with the setting for sampling clock.

Horizontal Position Use the left and right buttons to move the picture in horizontal direction while this option is selected.

Vertical P osition Use the left and right buttons to m ove the picture in vertical direction while this option is selected.

Reset this Mode Reset mode specific settings (Clock , Phase and Position) to the factory-made defaults.

Reset all Modes Reset all settings to the factory-made defaults.

Save changes Save changes permanently

Undo Changes Restore last settings

• **Refresh Video**

Click to run this menu item for retrieving the whole video again from the controlled host and displayed on Remote Console. In normal situation, only changed parts of video will be packed and sent from IP-101, for saving network bandwidth. This function is mainly used for troubleshooting purpose wher e some old video frag ments are displayed as not updated in time for some reason; for example, noise filter for VGA is setting too large.

• Soft Keyboard

Figure 4-8 Soft Keyboard

Opens up the Menu for the Soft-Keyboard.

• Show

Pops up the Soft-Keyboard. The Soft-Keyboard is necessary in case your host system runs a com pletely different language and country mapping than your adm inistration machine.

• Mapping

Used for choosing the specific language and country mapping of the Soft-Keyboard.

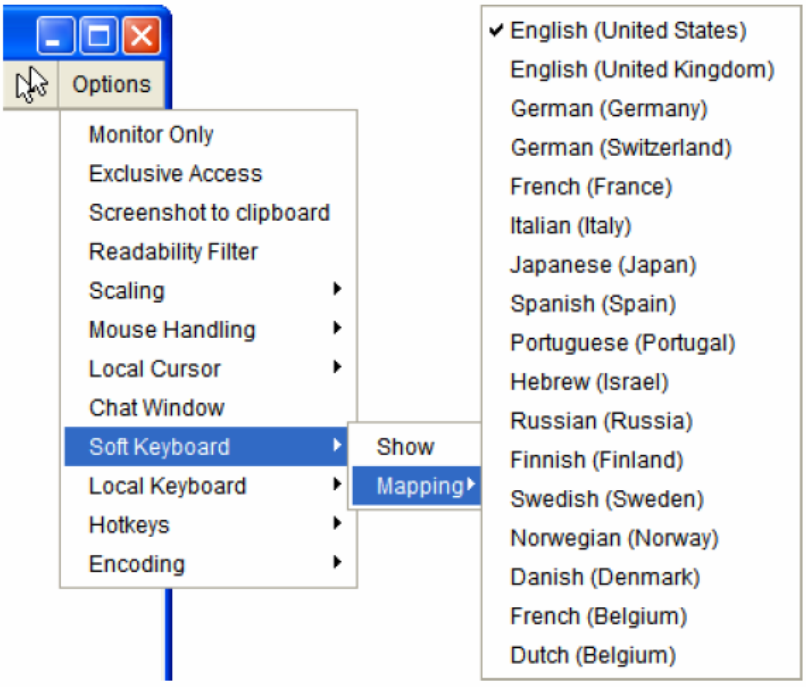


Figure 4-9 Soft Keyboard Mapping

• **Local Keyboard**

Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a German localized system that uses an US-English keyboard mapping. In this case you have to change the Local Keyboard setting to the right language, manually.

• **Hotkeys**

Opens a list of hotkeys defined before. Choose one entry, the command will be sent to the host system.

A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Select "OK" to execute the command on the remote host.

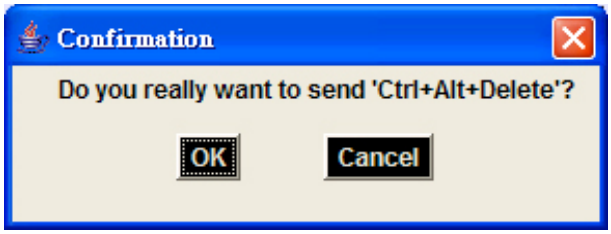


Figure 4-10 Remote Console Confirmation Dialog

• **Encoding**

These options are used to adjust the encoding level in terms of compression and color depth. They are only available unless "Transmission Encoding" is determined automatically (see the Section called *Transmission Encoding* in Chapter 6).

Compression Level:

you may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the best compression. The most suitable compression level should always be seen as a compromise between the network bandwidth that is available, on your video picture to be transferred, and on the number of changes between two single video pictures. We recommend to use a higher compression level if the network bandwidth is low. The higher the compression level the more time is needed to pack and unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g. the number of the colors or the diversity of pixels. The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture.

If level 0 is chosen the video compression is disabled, completely.

The option "Video Optimized" has its advantages if transferring high-quality motion pictures. In this case the video compression is disabled, completely and all video data is transferred via network as full-quality video snippets. Therefore, a high amount of bandwidth is required to ensure the quality of the video picture.

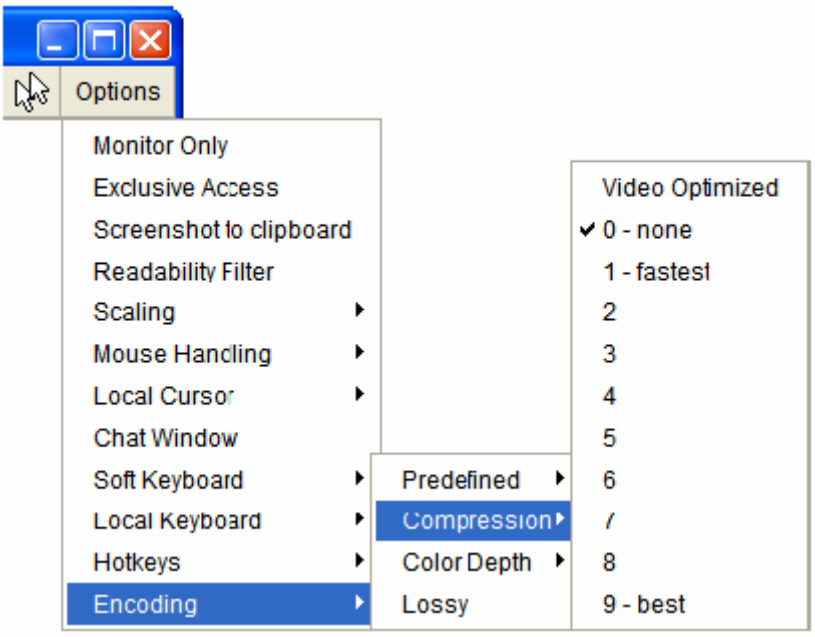


Figure 4-11 Encoding Compression

The next two options allow you to set the compression level to a predefined level OR to set a level for "lossy" compression. This compresses well, but leads to a degradation in image quality.

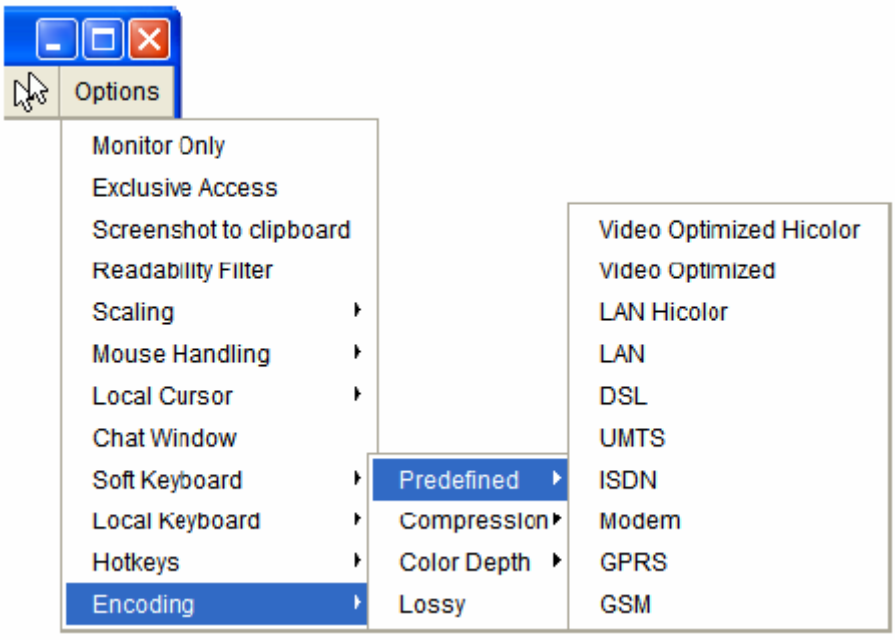


Figure 4-12 Predefined Compression

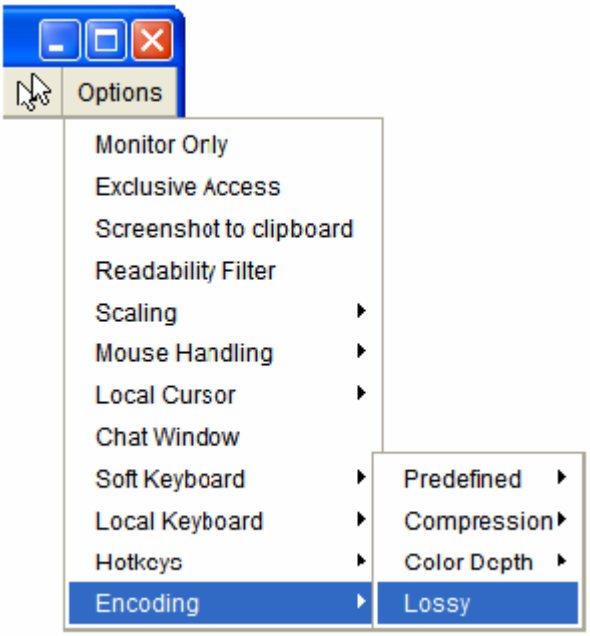


Figure 4-13 Lossy Compression

Color Depth:

set the desired color depth. You may select between 8 or 16 bit for Video Optimized/compression level 0, or between 1 and 8 bit for compression level 1 to 9. The higher the color depth, the more video information has to be captured and to be transferred.

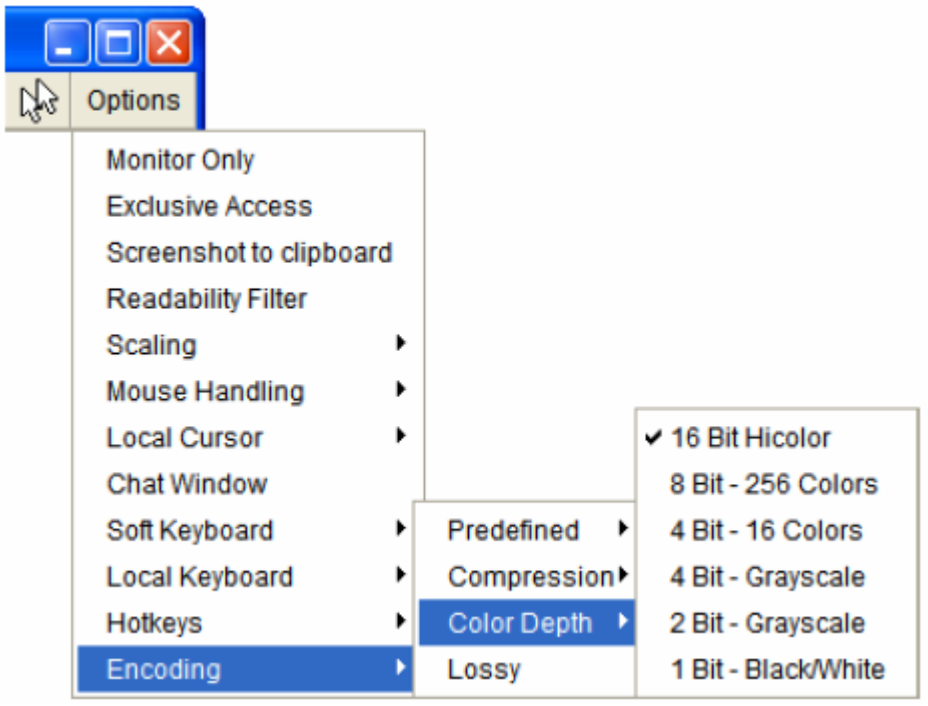


Figure 4-14 Encoding Color depth

Note: If displaying motion pictures on a connection with low speed you may achieve an improvement regarding the video transfer rate by lowering the color depth and disabling the option "Video Optimized". As a general result, the data rate is reduced (less bits per color). Furthermore, the OPMA module will not have to do any video compression. In total, this will lead to less transfer time of the motion picture.

4.3.3 Status Line of Remote Console

Status line

Shows both console and the connection state. The size of the remote screen is displayed. Figure belowwas taken from a Remote Console with a resolution of 800x600 pixels. The value in brackets describes the connection to the Remote Console. “Norm” means a standard connection without encryption, “SSL” means a secure connection.

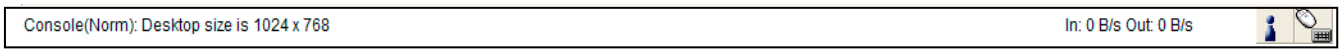


Figure 4-15 Status line

Furthermore, both the incoming (“In:”) and the outgoing (“Out:”) network traffic are visible (in kb/s). If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.

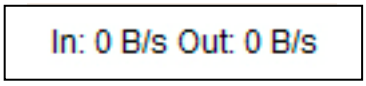
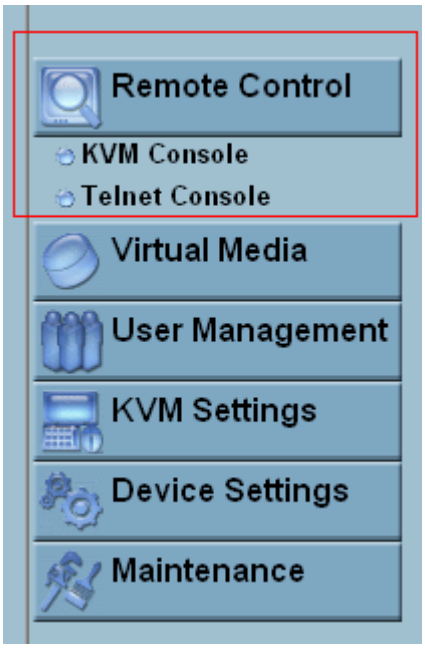


Figure 4-16 Status line transfer rate

For more information about Monitor Only and Exclusive Access settings, see related sections.

5. Menu Options

5.1 Remote Control



The Remote Console is the redirected screen, keyboard and mouse of the remote host system that IP-101 controls. The Remote Console window is a Java Applet that tries to establish its own TCP connection to the IP-101.

Starting the Remote Console opens a new window displays screen movement of host system, with its size automatically adjusted to optimum. Keyboard and mouse are redirected to control the host system simultaneously. A slight delay may present depending on the bandwidth of network.

5.1.1 KVM Console

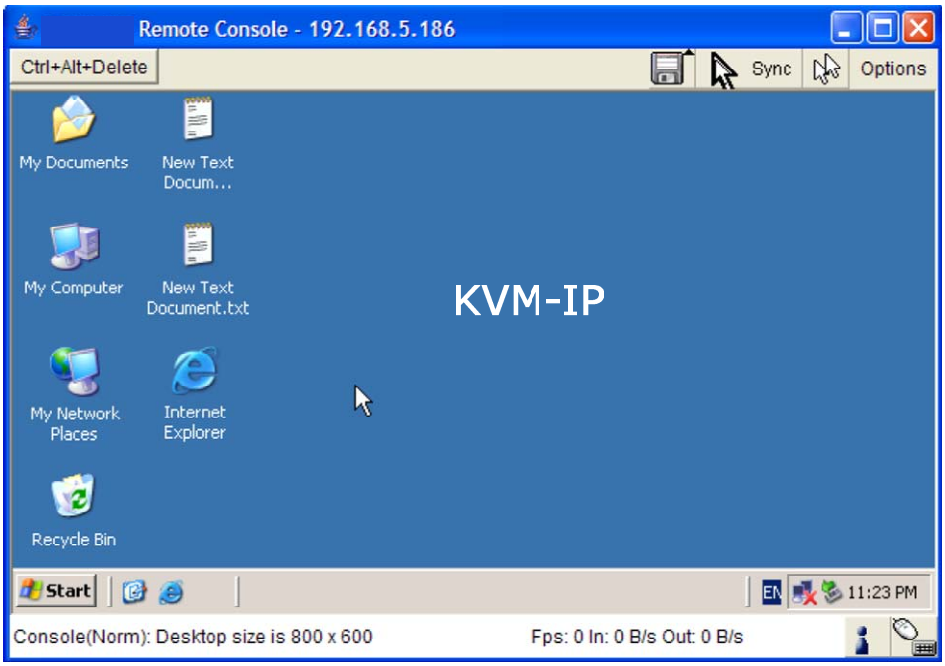


Figure 5-1 KVM Console

To open the KVM console either click on the icon **Console** or **Remote Control > KVM Console** of the menu entry on the left or **Click to open** of the console picture on the right.

5.1.2 Telnet Console

Figure 5-2 Telnet Console

The IP-101 firmware features a Telnet server that enables a user to connect via a standard Telnet client. In case the Telnet program is using a VT 100, VT 102 or VT 220 terminal or an according emulation, it is even possible to perform a console redirection as long as the IP-101 host machine is using a text mode screen resolution.

Connecting to the IP-101 is done as usual and as required by the Telnet client, for instance in a UNIX shell:

telnet 192.168.0.70

Replace the IP address by the one that is actually assigned to the IP-101. This will prompt for username and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means, the user management of the Telnet interface is entirely controlled with the according functions of the web interface.

Once you have successfully logged into the IP-101 a command line will be presented and you can enter according management commands.

In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were configured accordingly). All inputs are redirected to the device on serial port 1 and its answers are displayed on the Telnet interface.

The following list shows the according command mode command syntax and their usage.

help

Displays the list of possible commands.

cls

Clears the screen.

quit

Exits the current session and disconnects from the client.

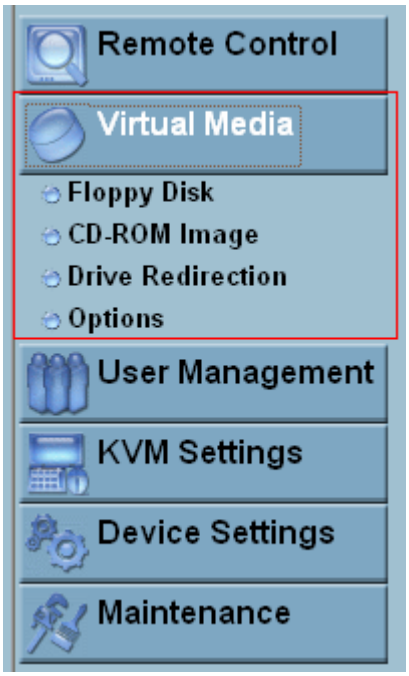
version

Displays the release information.

terminal

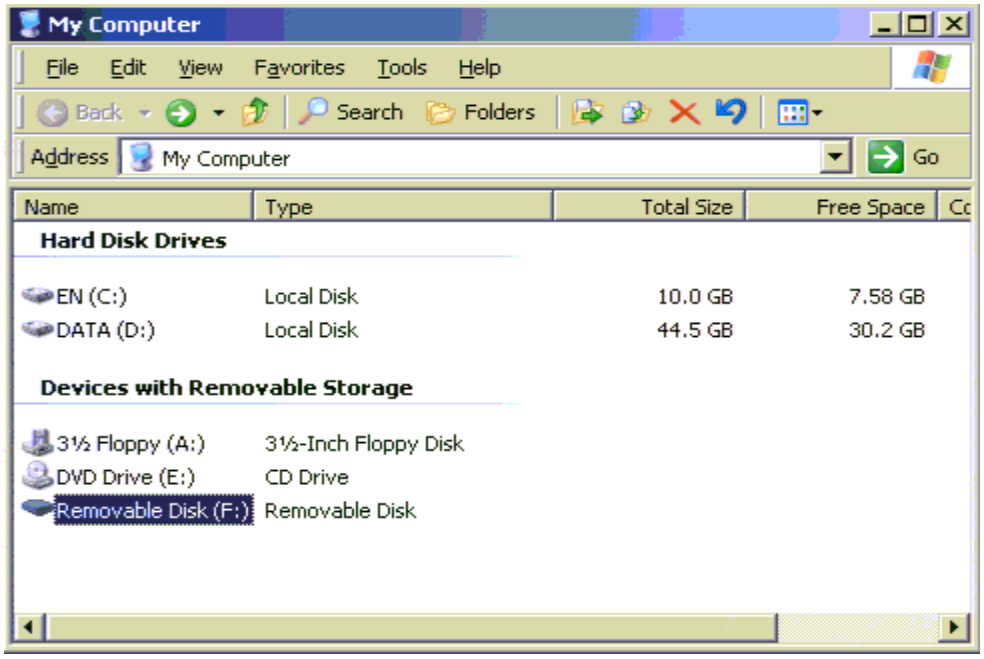
Starts the terminal passthrough mode for serial port 1. The key sequence *esc exit* switches back to the command mode.

5.2 Virtual Media



Before go ahead with this setup, both remote user computer and local computer (the one connected with I-BOX) would have to have Operating System Win2000, XP or above. This function would not work on other platforms at this moment.

Before using Virtual Media, please connect the USB cable from IP-101 to host computer. After connecting the USB cable, you can see a “Removable Disk” on the host computer. Below is the host computer screen (the computer which connected with IPKVM).


My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Go
Name Type Total Size Free Space
Hard Disk Drives
EN (C:) Local Disk 10.0 GB 7.58 GB
DATA (D:) Local Disk 44.5 GB 30.2 GB
Devices with Removable Storage
3½ Floppy (A:) 3½-Inch Floppy Disk
DVD Drive (E:) CD Drive
Removable Disk (F:) Removable Disk

5.2.1 Floppy Disk

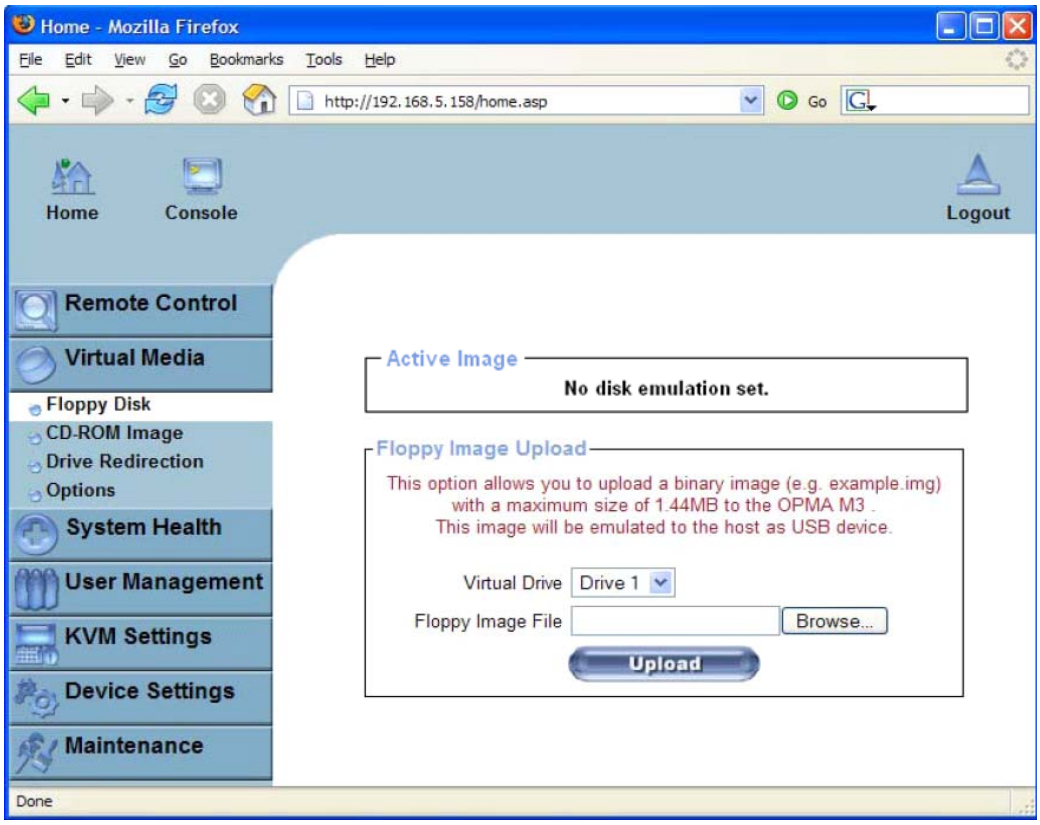
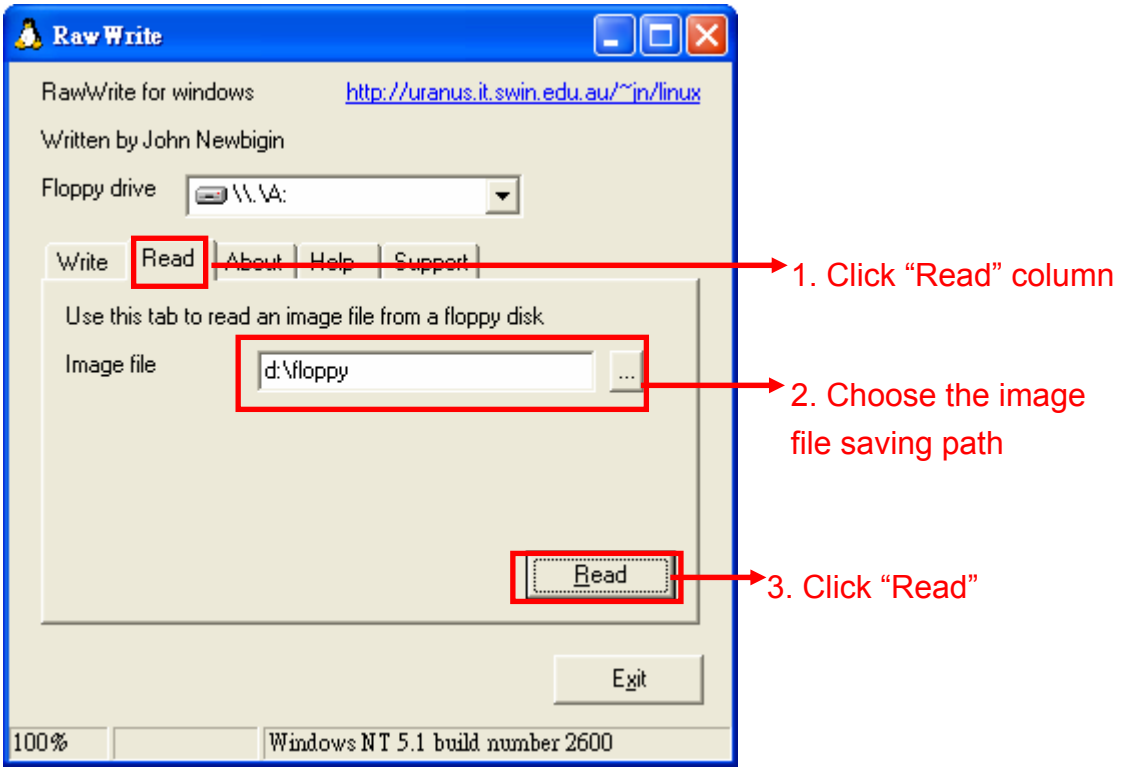
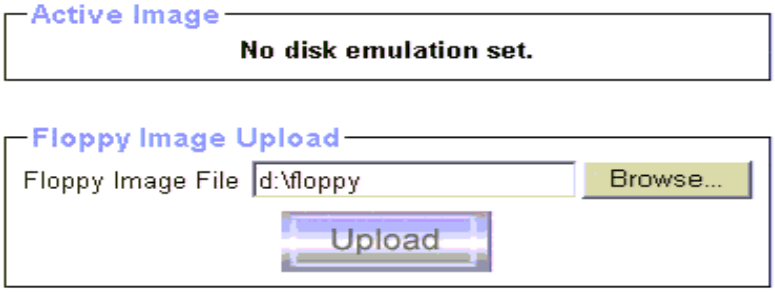


Figure 5-3 Virtual Media - Floppy Disk

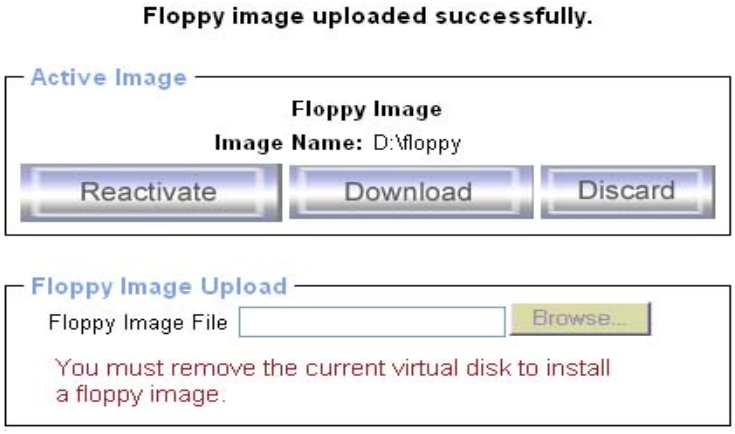
1. You need to create the floppy to an image file first.
2. For this example, we use RawWrite software (or any other image-creator software) to create floppy image. Please use licensed software for this purpose.



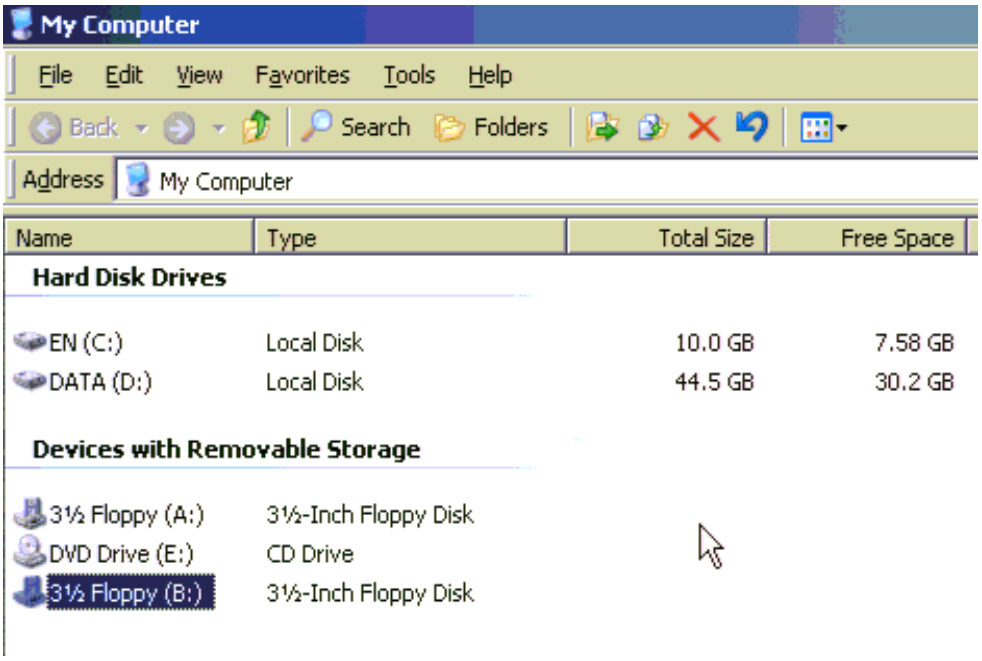
3. You can find a image file saved at desire destination after you created it with RawWrite.
4. Open the browser to log into the IP-101. Click **Virtual Media > Floppy Disk.** Click the Browse button to choose the image file.



5. After you uploading the image file, you will see the information below.



6. Open the remote console and you will see a virtual Floppy drive is created on the host computer that connect to IP-101.


My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Name Type Total Size Free Space
Hard Disk Drives
EN (C:) Local Disk 10.0 GB 7.58 GB
DATA (D:) Local Disk 44.5 GB 30.2 GB
Devices with Removable Storage
3½ Floppy (A:) 3½-Inch Floppy Disk
DVD Drive (E:) CD Drive
3½ Floppy (B:) 3½-Inch Floppy Disk

You may create a floppy image size up to 1.44Mb. This drive would be in read-only mode and would not allow you to write any information on this drive but copying only. This drive would be bootable under DOS mode if the motherboard/BIOS on the host computer supporting USB BOOTABLE function.

Notes:

1. If using other image-creator software, the output image extension file name has to be 'img', e.g. floppy_vir.img.
2. The uploaded image file will be kept in the onboard memory of the IP-101 until the end of the current session, as you logged out, or initiated a reboot of the IP-101.

5.2.2 CD–ROM Image

Use Image on Windows Share (SAMBA)

To include an image from a Windows share, select "CD-ROM" from the submenu.

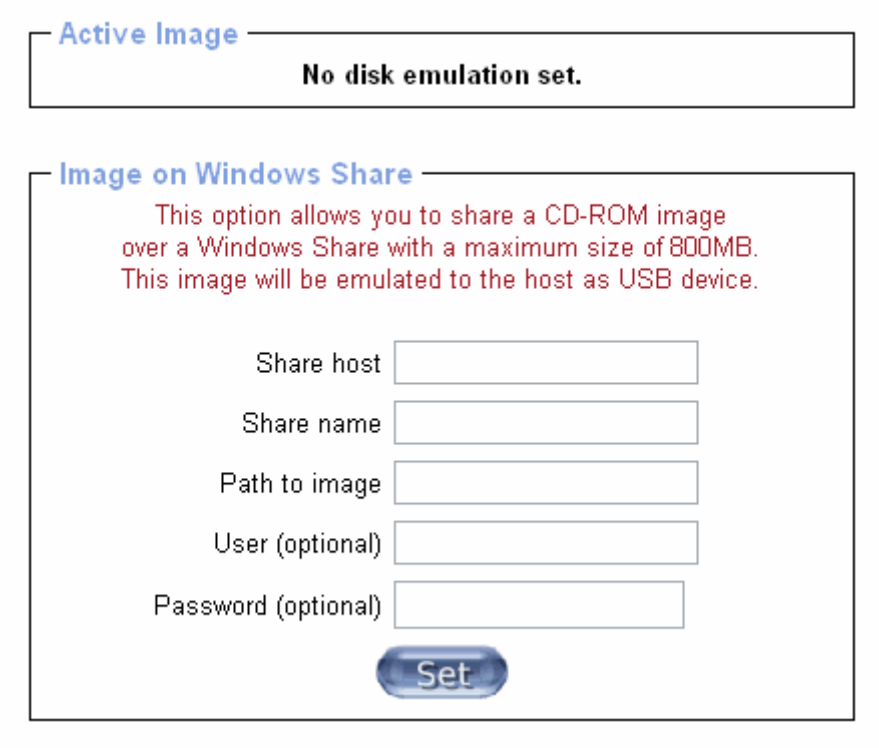

Active Image
No disk emulation set.
Image on Windows Share
This option allows you to share a CD-ROM image
over a Windows Share with a maximum size of 800MB.
This image will be emulated to the host as USB device.
Share host
Share name
Path to image
User (optional)
Password (optional)
Set

Figure 5-4 Virtual Media – CD-ROM Image

Operation Procedures:

1. Please run Nero or any CD imaging tool to create CD-ROM ISO image.
2. Please create a folder and share this folder. (Please make sure password has to be setup with the authorized user during Sharing => Permission settings)
3. Copy the CD-ROM ISO image file to this sharing folder.
4. Please fill in the sharing information as below picture.

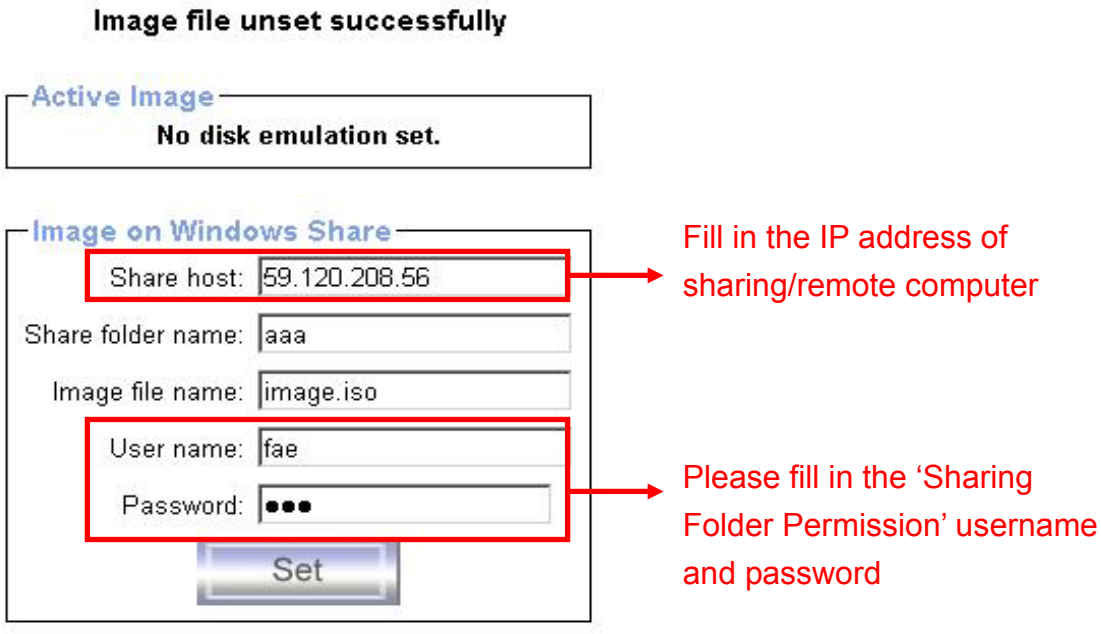
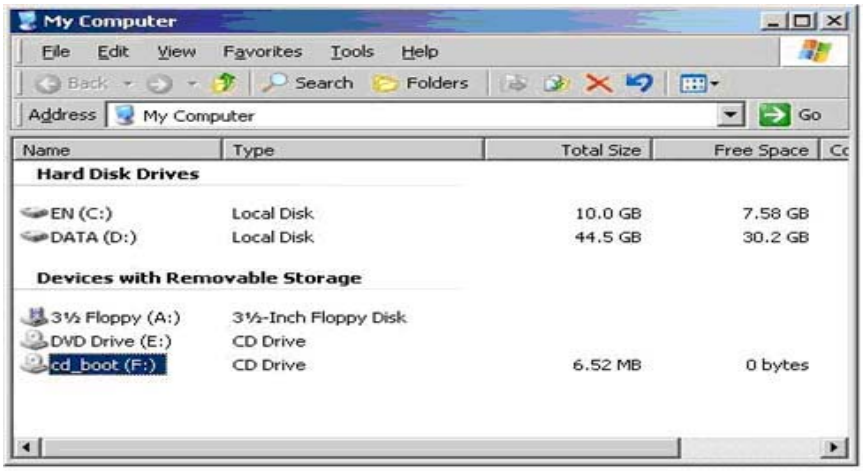


Image file unset successfully
Active Image
No disk emulation set.
Image on Windows Share
Share host: 59.120.208.56
Share folder name: aaa
Image file name: image.iso
User name: fae
Password:
Set
Fill in the IP address of sharing/remote computer
Please fill in the 'Sharing Folder Permission' username and password

5. Image file set successfully.

6. Open the remote console, you can see the virtual CD as below picture.


My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Go
Name Type Total Size Free Space
Hard Disk Drives
EN (C:) Local Disk 10.0 GB 7.58 GB
DATA (D:) Local Disk 44.5 GB 30.2 GB
Devices with Removable Storage
3½ Floppy (A:) 3½-Inch Floppy Disk
DVD Drive (E:) CD Drive
cd_boot (F:) CD Drive 6.52 MB 0 bytes

Note: the output image extension file name has to be 'iso', e.g. CD-Rom_vir.iso.
You may create an ISO image size up to 650Mb. This drive would be in read-only mode and would not allow you to write any information on this drive but copying only. This drive would be bootable under DOS mode if the motherboard/BIOS on the host computer supports USB BOOTABLE function. For emulating DVD Drive, please use **Drive Redirection** function.

Note: The above information has to be given from the point of view of IP-101 with correct IP address and device name. Administrative permission is required as regular user may not have the right to access. Please login as a system administrator (or as "root" on UNIX systems).

The following information has to be given to mount the image properly:

Share host -- The server name or its IP address.

Share folder name -- The name of the share folder to be used.

Image file name -- The name of the image file on the share folder.

User name -- If necessary, specify the user name for the share named in advance. If unspecified, and a guest account is activated, this guest account information will be used as your login.

Password -- If necessary, specify the password for the given user name.

To register the specified file image and its location click on the button “Set”.

The specified image file is supposed to be accessible from the IP-101. The information above has to be given from the point of view of the IP-101. It is important to specify correct IP addresses, and device names. Otherwise, IP-101 may not be able to access the referenced image file.

Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these perm issions. You should either log in as a system administrator (or as “root” on UNIX systems), or ask your system administrator for help to complete this task.

MS Windows

Open the Explorer, navigate to the directory (or share), and press the right mouse button to open the context menu.

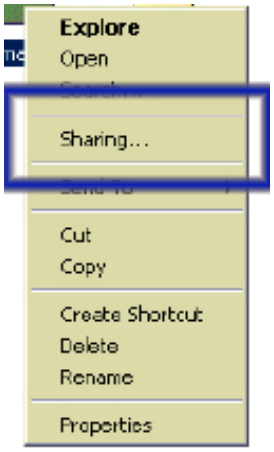


Figure 5-5 Explorer context menu

Select “Sharing” to open the configuration dialog.

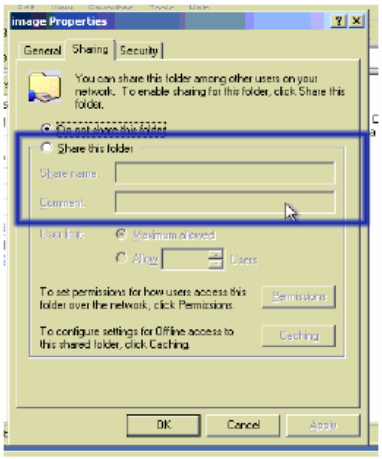


Figure 5-6 Share configuration dialog

Adjust the settings for the selected directory.

- Activate the selected directory as a share. Select “Sharing this folder”.
- Choose an appropriate name for the share. You may also add a short description for this folder (input field “Comment”).
- If necessary, adjust the permissions (button “permissions”).
- Click “OK” to set the options for this share.

UNIX and UNIX-like OS (Sun Solaris, and Linux)

If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file /etc/samba/smb.conf, or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

5.2.3 Drive redirection

The Drive Redirection is another possibility to use a virtual disc drive on the remote computer. With Drive Redirection you do not have to use an image file but may work with a drive from your local computer on the remote machine. The drive is hereby shared over a TCP network connection. Devices such as floppy drives, hard discs, CD ROMs and other removable devices like USB sticks can be redirected. It is even possible to enable a write support so that for the remote machine it is possible to write data to your local disc.

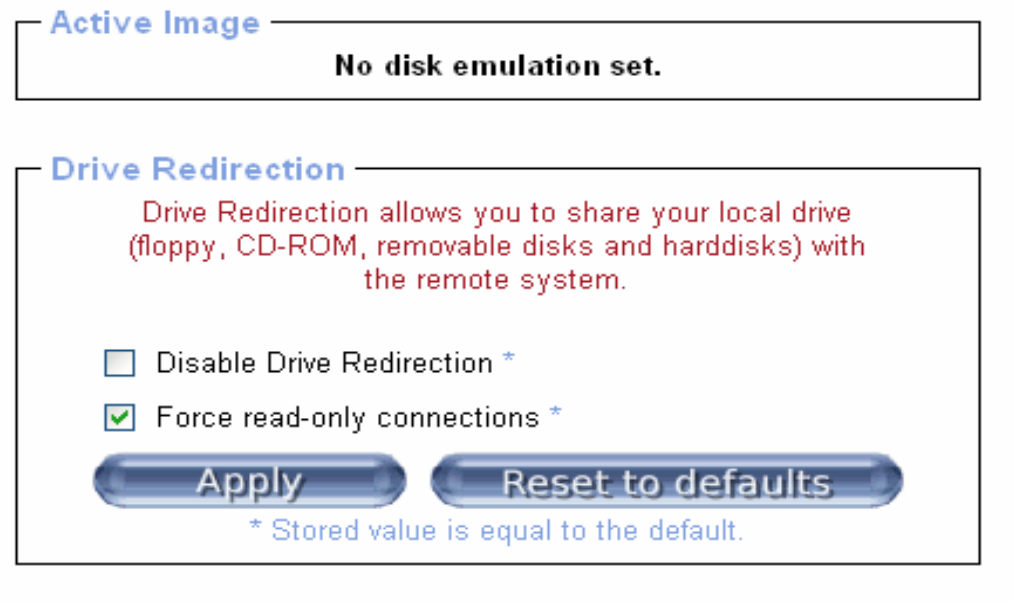

Active Image
No disk emulation set.
Drive Redirection
Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.
Disable Drive Redirection *
Force read-only connections *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 5-7 Options of Drive Redirection

Please note that Drive Redirection works on a level which is far below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected, actually. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine, or from the remote host) is writing data on the device. If write support is enabled the remote computer might damage the data and the file system on the redirected device. On the other hand, if the local operating system writes data to the redirected device the drive cache of the operating system of the remote host might contain older data. This may confuse the remote host's operating system . We recommend to use the Drive Redirection with care, especially the write support.

Disable Drive Redirection

If enabled the Drive Redirection is switched off.

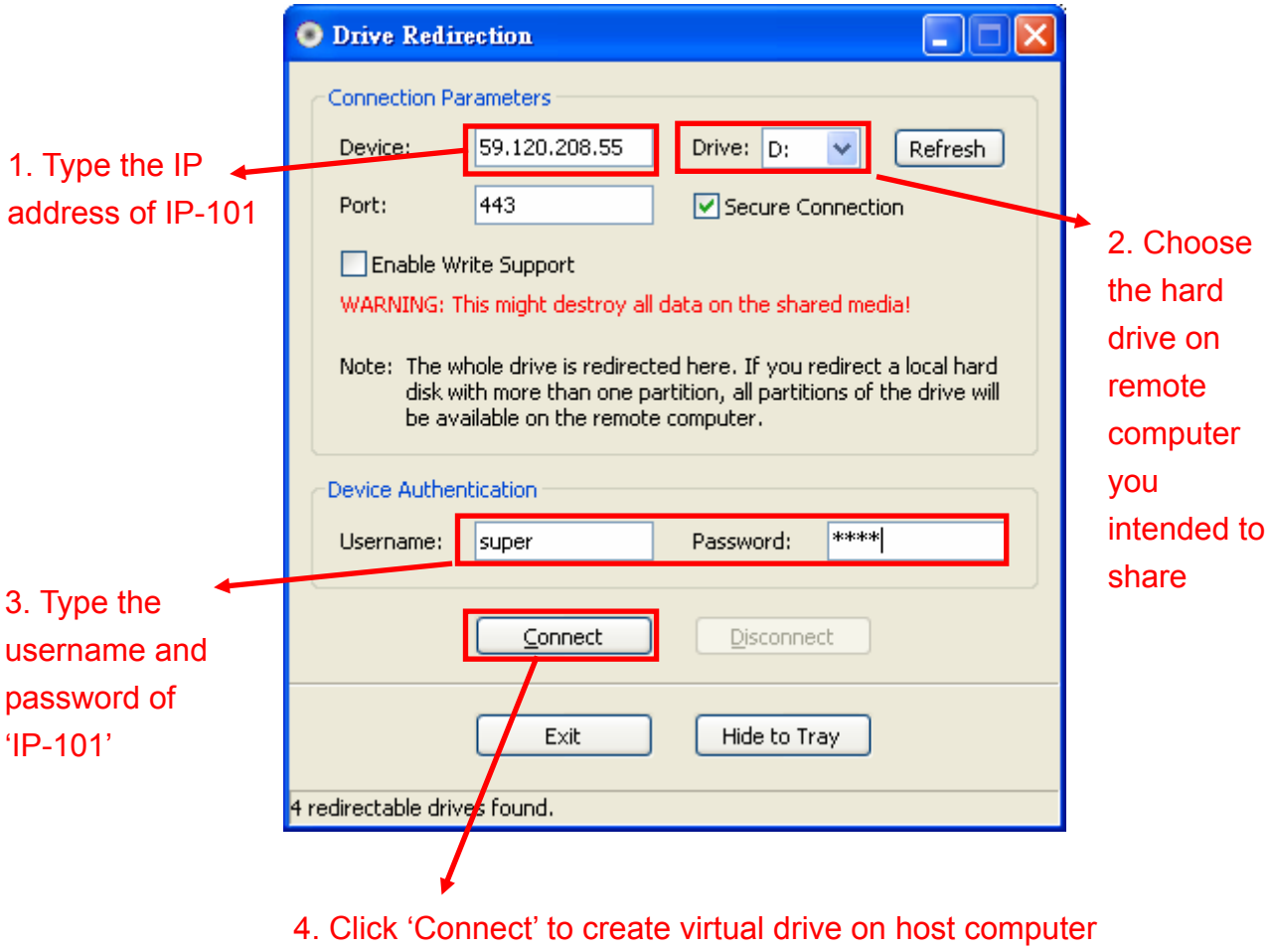
Force read-only connections

If enabled the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.

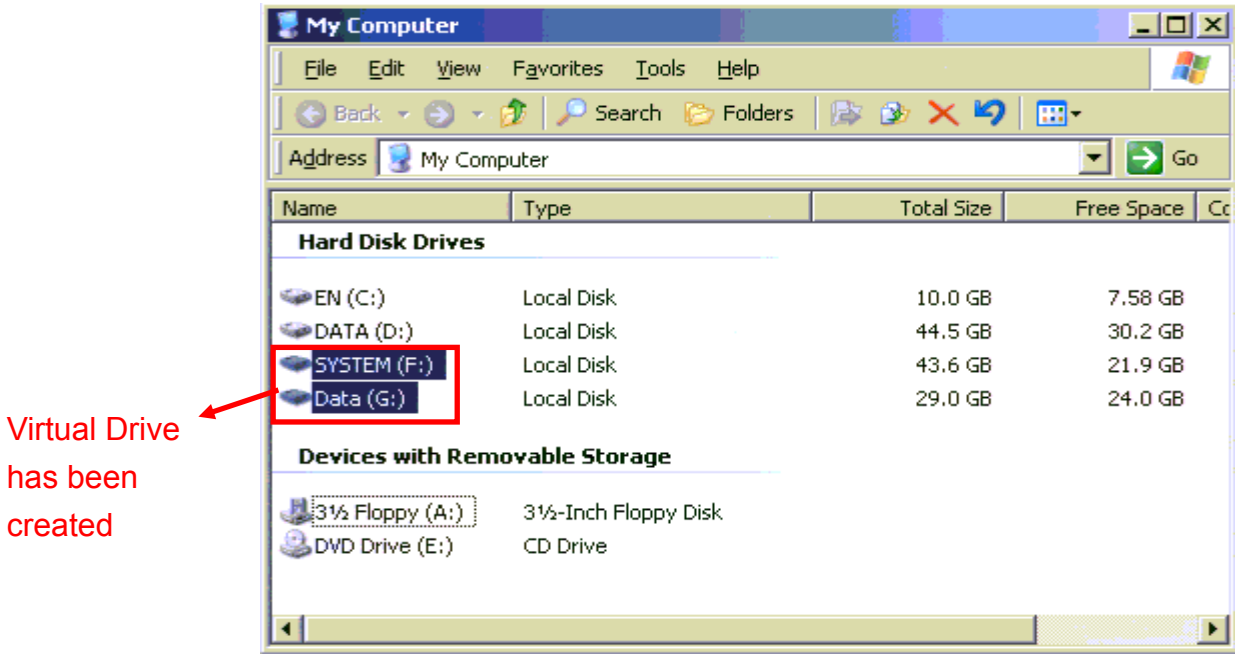
Click **Apply** to submit your changes.

Operation Procedures:

1. Please install Drive Redirection Software on remote computer first then run Drive Rediection application and fill in information accordingly:


Drive Redirection
Connection Parameters
Device: 59.120.208.55
Drive: D:
Refresh
Port: 443
Secure Connection
Enable Write Support
WARNING: This might destroy all data on the shared media!
Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.
Device Authentication
Username: super
Password: ****
Connect
Disconnect
Exit
Hide to Tray
4 redirectable drives found.
1. Type the IP address of IP-101
2. Choose the hard drive on remote computer you intended to share
3. Type the username and password of 'IP-101'
4. Click 'Connect' to create virtual drive on host computer

2. Open the remote and you can see the virtual hard drive as below picture.


My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Go
Name Type Total Size Free Space
Hard Disk Drives
EN (C:) Local Disk 10.0 GB 7.58 GB
DATA (D:) Local Disk 44.5 GB 30.2 GB
SYSTEM (F:) Local Disk 43.6 GB 21.9 GB
Data (G:) Local Disk 29.0 GB 24.0 GB
Devices with Removable Storage
3½ Floppy (A:) 3½-Inch Floppy Disk
DVD Drive (E:) CD Drive
Virtual Drive has been created

Please note that Virtual Drive creation is by Device manner not by Partition. Which means it looks for I/O in BIOS and sends the corresponding signal to host computer. This way, you are sending the entire hard drive (may consist of 'X' numbers of partitions) and emulate whatever

number of partitions on host computer. You may also emulate a DVD-Drive with the same procedure. However, this DVD-Drive **Does NOT** support Bootable function like Floppy and CD-Rom emulation.

There are two methods of Drive Redirections:

1. External Drive Redirection Utility
2. Built-in Java Drive Redirection function in Remote Console

5.2.3.1 Driver Redirection Utility Installation

Please follow the Drive Redirection Setup Wizard step by step to install the driver from the attached CD ROM.

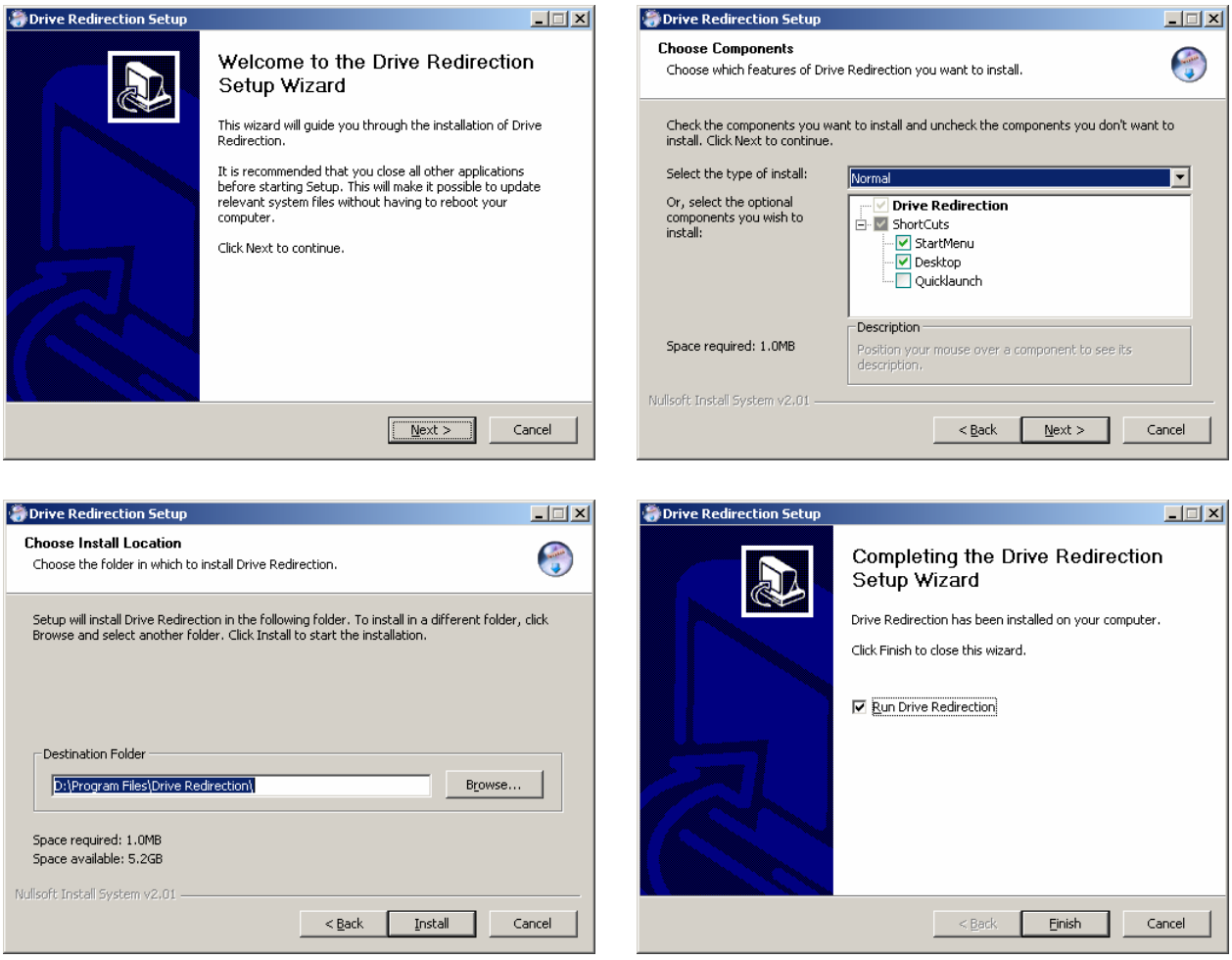

Drive Redirection Setup
Welcome to the Drive Redirection Setup Wizard
This wizard will guide you through the installation of Drive Redirection.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel
Drive Redirection Setup
Choose Components
Choose which features of Drive Redirection you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Normal
Or, select the optional components you wish to install:
Drive Redirection
ShortCuts
StartMenu
Desktop
Quicklaunch
Description
Position your mouse over a component to see its description.
Space required: 1.0MB
Nullsoft Install System v2.01
< Back
Next >
Cancel
Drive Redirection Setup
Choose Install Location
Choose the folder in which to install Drive Redirection.
Setup will install Drive Redirection in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
D:\Program Files\Drive Redirection\
Browse...
Space required: 1.0MB
Space available: 5.2GB
Nullsoft Install System v2.01
< Back
Install
Cancel
Drive Redirection Setup
Completing the Drive Redirection Setup Wizard
Drive Redirection has been installed on your computer.
Click Finish to close this wizard.
Run Drive Redirection
< Back
Finish
Cancel

Figure 5-8 Drive Redirection Setup

Drive Redirection Settings

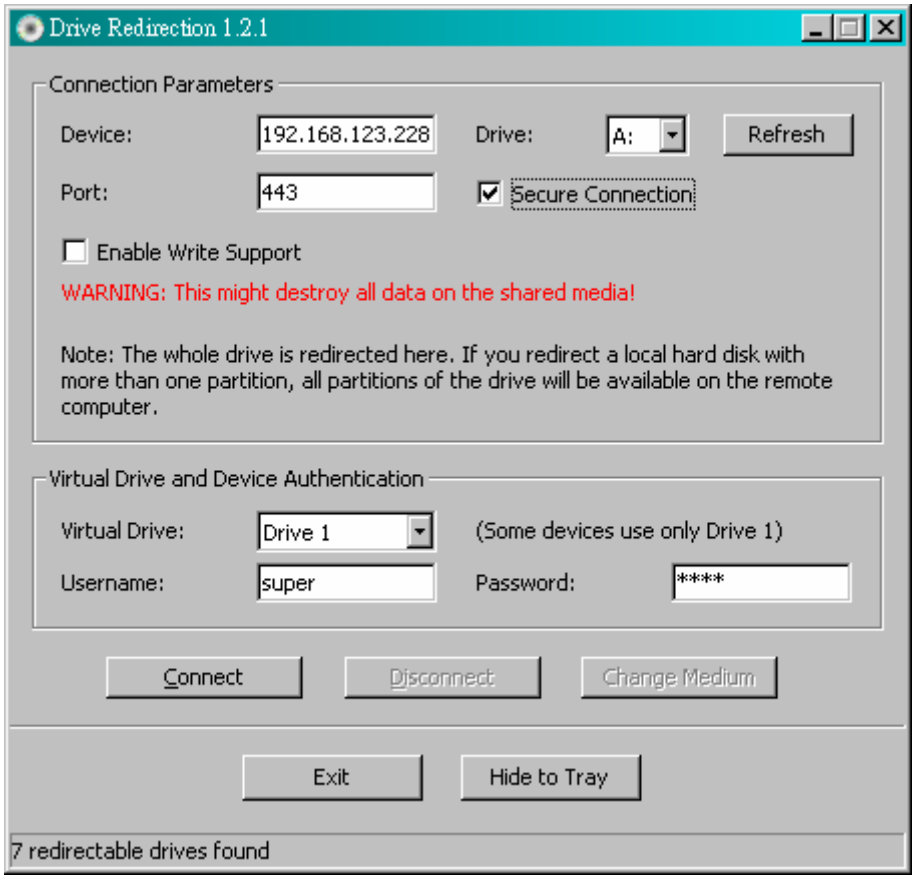


Figure 5-9 Drive Redirection dialog

Drive Redirection Utility:

Device

This is the address (either the DNS name or the IP address) of the IP-101 you would like to connect to.

Drive

The local drive you want to share with the remote computer, which could be Floppy disc, CD-ROMs, USB-Sticks and hard drives.

Port

This is the network port. By default, IP-101 uses the remote console port (#443) here. You may change this value if you have changed the remote console port in your IP-101's network settings.

Secure Connection

Enable this box to establish a secure connection via SSL. This will maximize the security but may reduce the connection speed.

Select the drive you would like to redirect. All available devices (drive letters) are shown here. Please note that the whole drive is shared with the remote computer, not only one partition. If you have a hard disc with more than one partition all drive letters that belong to this disc will be redirected. The Refresh button may be used to regenerate the list of drive letters, especially for an USB stick.

Warning

Please be cautious that if "Allow Write Support" is selected, all data on the shred media might be destroyed.

Write Support

This feature may be enabled here. Write support means that the remote computer is allowed to write on your local drive. As you can imagine, this is very dangerous. If both the remote and the local system try to write data on the same device, this will certainly destroy the file system on the drive. Please use this only when you exactly know what you are doing.

Device Authentication

The factory default Username is "super" and the default Password is "pass".
Click **Connect** to redirect drive

Warning

1. Drive Redirection is only possible with Windows 2000 or above versions.
2. The Drive Redirection w orks on a low SCSI le vel and the SC SI protocol cannot recognize partitions; theref ore the whole drive selected will be shared instead of any particular partition.
3. While connecting to a legacy KVM switch, please select PS/2 mouse for **Keyboard/Mouse setting** from webpage. Otherwise you will not be able to use Hot-key.

Navigation Buttons:

Connect/Disconnect

To establish the drive redirection please press the **Connect** button once. If all the settings are correct, the status bar displays that the connection has been established, the Connect button is

disabled and the Disconnect button is enabled.

On an error, the status line shows the error message. The drive redirection software tries to lock the local drive before it is redirected. That means that it tries to prevent the local operating system from accessing the drive as long as it is redirected. This may also fail, especially if a file on the drive is currently open. In the case of a locking failure, you will be prompted if you want to establish the connection anyhow. This should not be a serious problem when the note above is respected. If the write support is enabled, a drive which is not locked might be damaged by the Drive Redirection.

With the **Disconnect** button, a connection via Drive Redirection connection is stopped.

Exit/Hide

If the **Exit** button is pressed, the Drive Redirection software is closed. If a Drive Redirection connection is active, the connection will be closed before the application terminates.

Using the Hide to Tray button the application is hidden, but not terminated completely. That means that an active connection will be kept active until it is closed explicitly. You can access the software by its tray icon. The tray icon also shows whether a connection is established or not. A double click on the icon shows the application window, or with a right click you may access a small menu

5.2.3.2 Built-in Java Drive Redirection

1. Run Remote Control > KVM Console.

2. Click “Floppy” icon

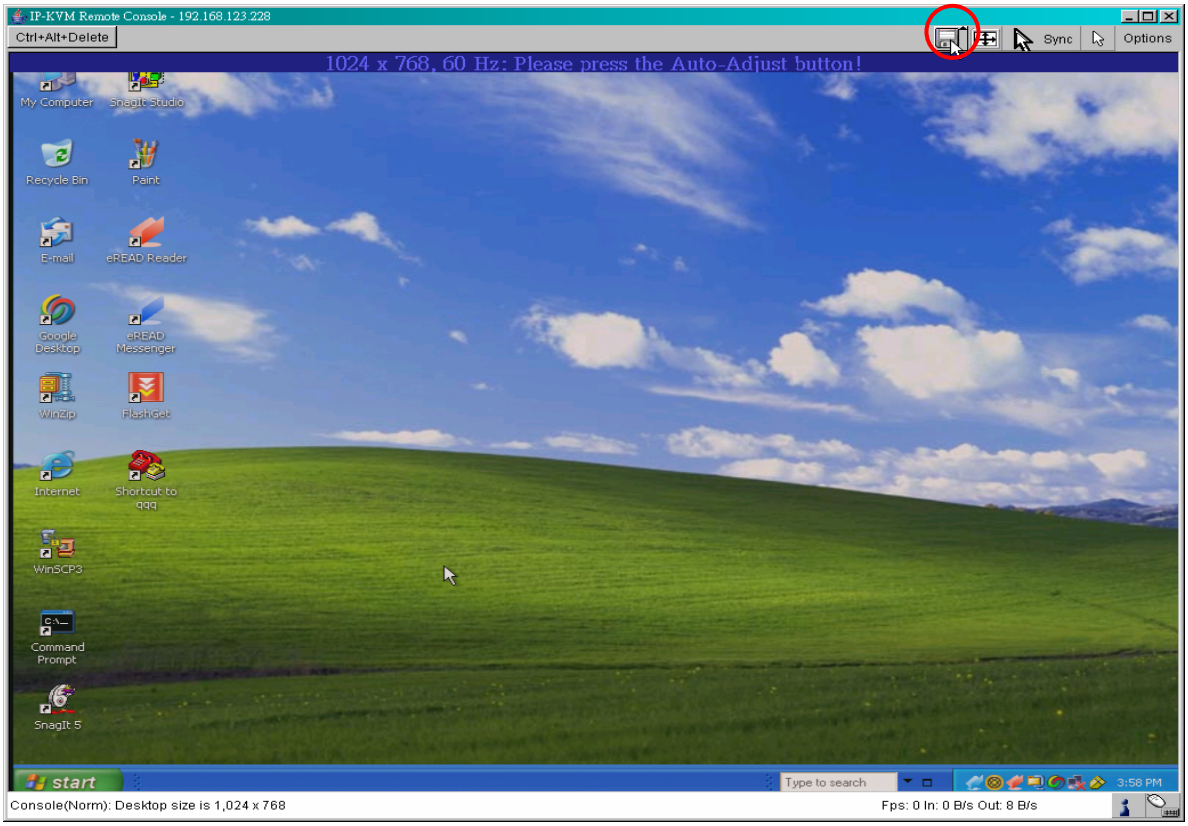
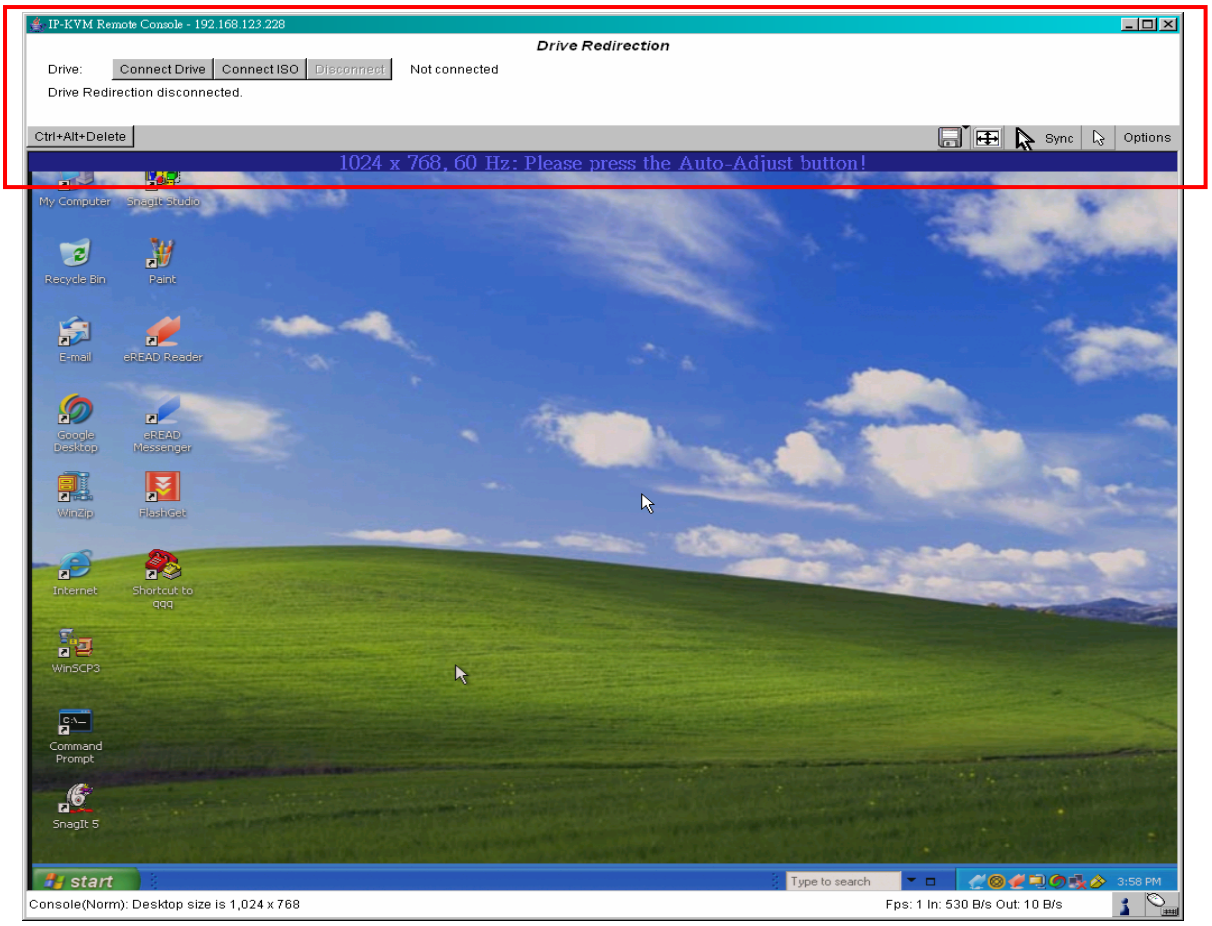
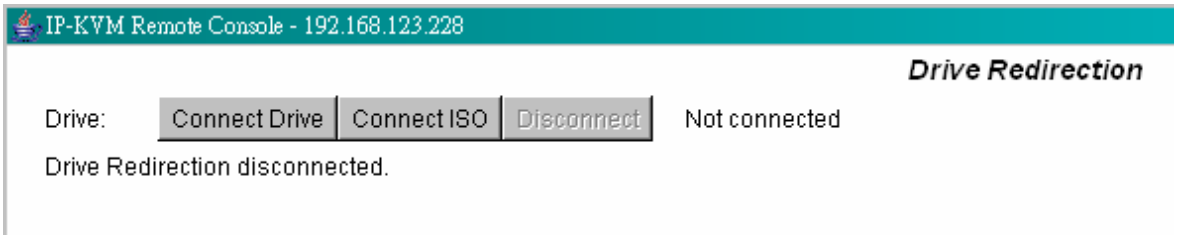


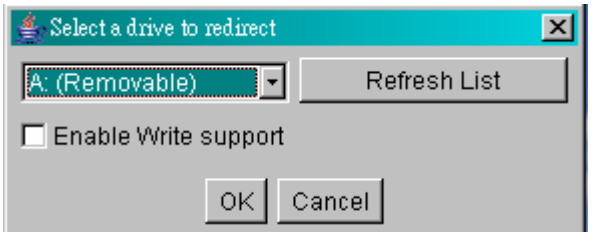
Figure 5-10 Built-in Java Drive Redirection

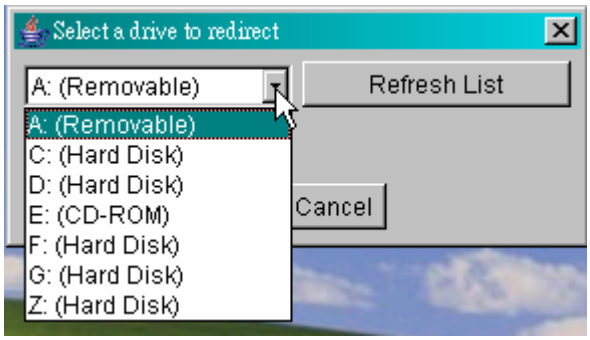


3. Click **Connect Drive** or **Connect ISO**



4. Select a drive to redirect (if Connect Drive)





5. Select a ISO image to redirect (if Connect ISO)

5.2.4 Options

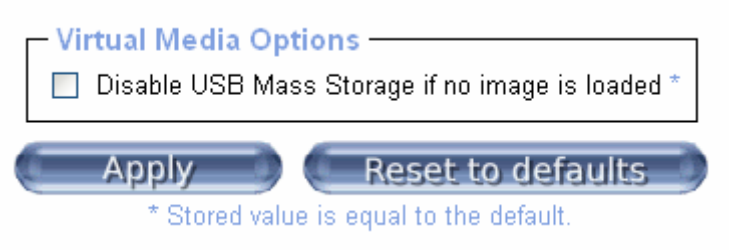

Virtual Media Options
Disable USB Mass Storage if no image is loaded *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 5-11 USB mass storage option

Set this option to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. If unset, and no file image will be found it may happen that the host system will hang on boot due to changes in the boot order, or the boot manager (LILO, GRUB). This case was reported for some Windows versions (2000, XP), other OS might not be fully excluded. This behavior depends on the BIOS version used in that machine.

To set this option, press the button “Apply”.

5.2.4.1 Creating an Image

5.2.4.1.1 Floppy Images

UNIX and UNIX-like OS

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

To create a floppy image file, copy the contents of a floppy to a file. You can use the following command:

dd [*if=/dev/fd0*] [*of=/tmp/floppy.image*]

dd reads the entire disc from the device /dev/fd0, and saves the output in the specified output file /tmp/floppy.image. Adjust both parameters exactly to your needs (input device etc.)

MS Windows

You can use the tool “Raw Write for Windows”. It is included on the CD ROM shipped with IP-101.

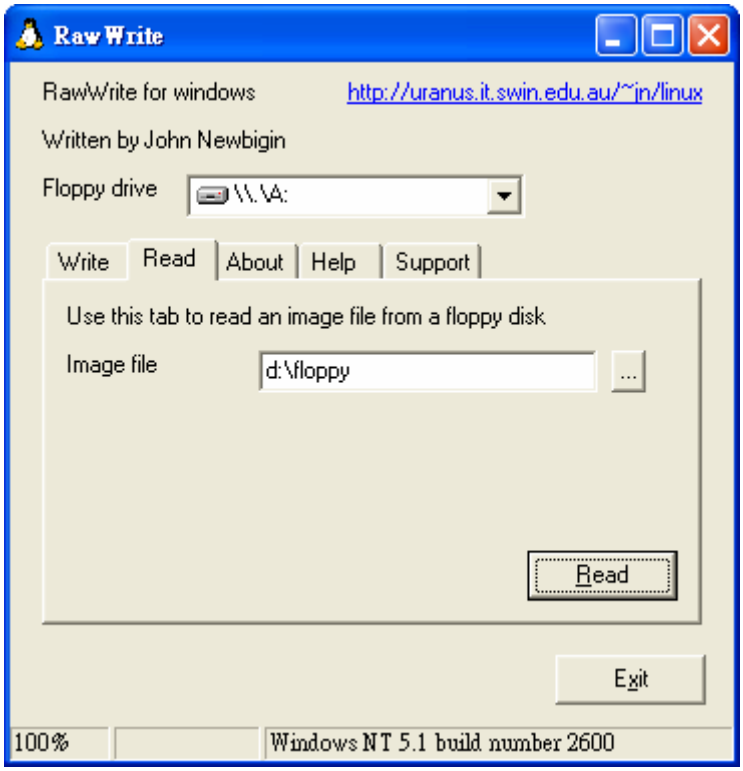


Figure 5-12 RawWrite for Windows selection dialog

From the menu, select the tab "Read". Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the button "Copy" to initiate the image creation process.

For related tools you may have a look at www.fdos.org

5.2.4.1.2 CD ROM/ISO Images

UNIX and UNIX-like OS

To create an image file, make use of "dd". This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

To create a CDROM image file, copy the contents of the CDROM to a file. You can use the following command:

dd [*if=/dev/cdrom*] [*of=/tmp/cdrom.image*]

dd reads the entire disc from the device /dev/cdrom, and saves the output in the specified output file /tmp/cdrom.image. Adjust both parameters exactly to your needs (input device etc.).

MS Windows

To create the image file, use your favorite CD imaging tool. Copy the whole contents of the disc into one single image file on your hard disk.

For example, with “Nero” you choose “Copy and Backup”. Then, navigate to the “Copy Disc” section. Select the CD ROM or DVD drive you would like to create an image from. Specify the filename of the image, and save the CD ROM content in that file.

Figure 5-13 Nero selection dialog

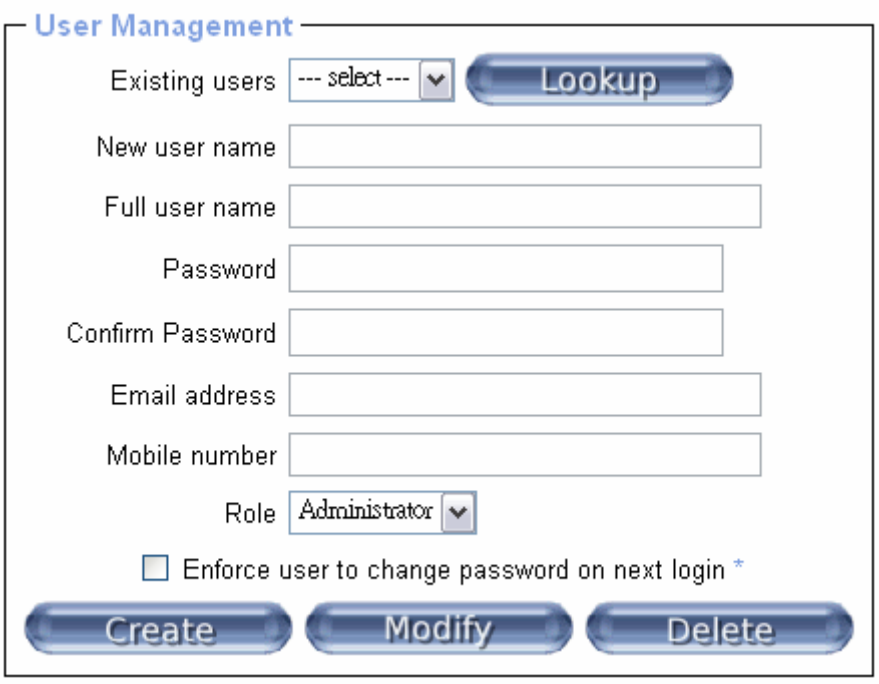
5.3 User Management

5.3.1 Change Password

Figure 5-14 Setting Password

Change password of currently logged in user:
Old Password: type in current password
New Password: type in new password
Confirm New Password: re-type new password for verification
Click “Apply” to submit your changes.

5.3.2 Users and Groups



There are three kinds of levels of user accounts:

- **Super --** Has all possible rights to configure the device
- **Administrator --** Has partial rights to change configuration apart from critical settings
- **User --** Has permission to access basic function of open Remote Console

You can choose the desired level from the selection box **role**.

The IP-101 comes with 1 pre-configured user account that has fixed permissions. The account “super” has all possible rights to configure the device and to use all functions IP-101 offers.

Upon delivery, the account “super” has the password “pass”. Make sure to change password immediately after you have installed and on initial access of your IP-101.

Existing users

Select an existing user for modification. Once a user has been selected, click the lookup button to see the user information.

New User name

The new user name for the selected account.

Password

The password for the login name. It must be at least three characters long.

Confirm password

Confirmation of the password above.

Email address

This is optional.

Mobile number

This information may be optionally provided.

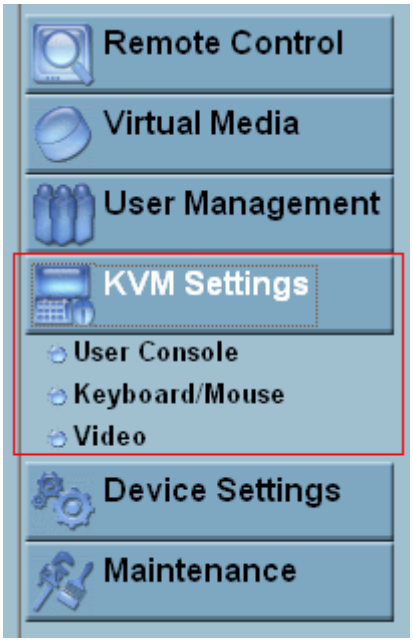
Role

Each user can be a member of a group (named a “role”) – there kinds can be shose from: super, administrator, or an regular user.

To create an user press the button **Create**. The **Modify** button changes the displayed user settings. To delete an user press the button **Delete**.

Note:The IP-101 is equipped with an host-independent processor and memory unit which both have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time we recommend not to exceed the number of 15 users connected to the IP-101 at the same time. The memory space that is available onto the IP-101 mainly depends on the configuration and the usage of the IP-101 (log file entries etc.). That’s why we recommend not to store more than 150 user profiles.

5.4 KVM Settings



5.4.1 User Console

The following settings are user specific. That means, the super user can customize these settings for every users separately. Changing the settings for one user does not affect the settings for the other users.

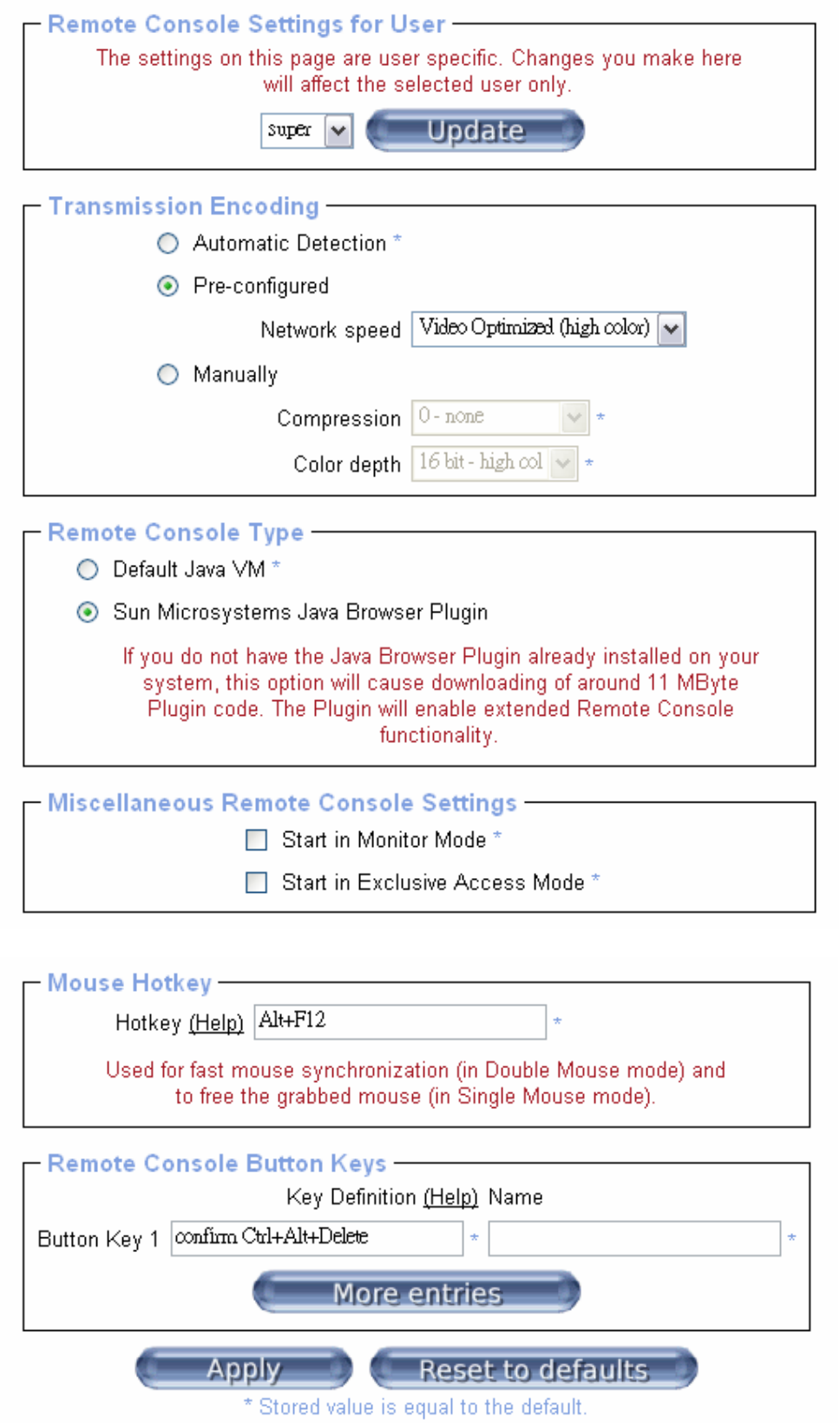

Remote Console Settings for User
The settings on this page are user specific. Changes you make here will affect the selected user only.
super
Update
Transmission Encoding
Automatic Detection *
Pre-configured
Network speed
Video Optimized (high color)
Manually
Compression
0 - none
Color depth
16 bit - high col
Remote Console Type
Default Java VM *
Sun Microsystems Java Browser Plugin
If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.
Miscellaneous Remote Console Settings
Start in Monitor Mode *
Start in Exclusive Access Mode *
Mouse Hotkey
Hotkey (Help)
Alt+F12
Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).
Remote Console Button Keys
Key Definition (Help)
Name
Button Key 1
confirm Ctrl+Alt+Delete
More entries
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 5-15 User Console Setting

User select box

This selection box displays the user ID for which the values are shown and for which the changes will take effect. You may change the settings of other users if you have the required privileges.

Transmission Encoding

The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen processing depending on the number of users working at the same time and the network bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

Automatic detection

The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

Pre-configured

The pre-configured settings deliver the best result because of optimized adjustment of compression and colour depth for the indicated network speed.

Manually

Allows to adjust both compression rate and the colour depth individually. Depending on the selected compression rate the data stream between the IP-101 and the Remote Console will be compressed in order to save bandwidth. Since high compression rates consum more computing power of IP-101, they should not be used while several users are accessing the IP-101 simultaneously.

The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

Remote Console Type

Specifies, which Remote Console Viewer to use.

Default Java-VM

Uses the default Java Virtual Machine of your Browser. This may be the Microsoft JVM for the Internet Explorer, or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plugin

Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java Applet. If you check this box for the first time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with “yes” . The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM lays in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for this JVM versions and offers wider range of functionality when run in SUN's JVM. Please make sure that you are installing Sun JVM 1.4.2 or above to your client system.

Miscellaneous Remote Console Settings

Start in Monitor Mode

Sets the initial value for the monitor mode. By default the monitor mode is off. In case you switch it on, the Remote Console window will be started in a read only mode.

Start in Exclusive Access Mode

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

Mouse hotkey

Allows to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console, or is used to leave the single mouse mode.

Remote Console Button Keys

Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact, that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are “Control+Alt+Delete” on Windows and DOS, what is always caught, or “Control+Backspace” on Unix or Unix-like OS for terminating the X-Server. The syntax to define a new Button Key is as follows:

[confir m] <keycode>[+|-[*]<keycode>]*

“confirm” requests confirmation by a dialog box before the key strokes will be sent to the remote host.

“keycode” is the key to be sent. Multiple key codes can be concatenated with a plus, or a minus sign. The plus sign builds key combinations, all keys will be pressed until a minus sign or the end of the combination is encountered. In this case all pressed keys should be

released in reversed sequence. The minus sign builds single, separate key presses and releases. The star inserts a pause with duration of 100 milliseconds.

5.4.2 Keyboard/Mouse

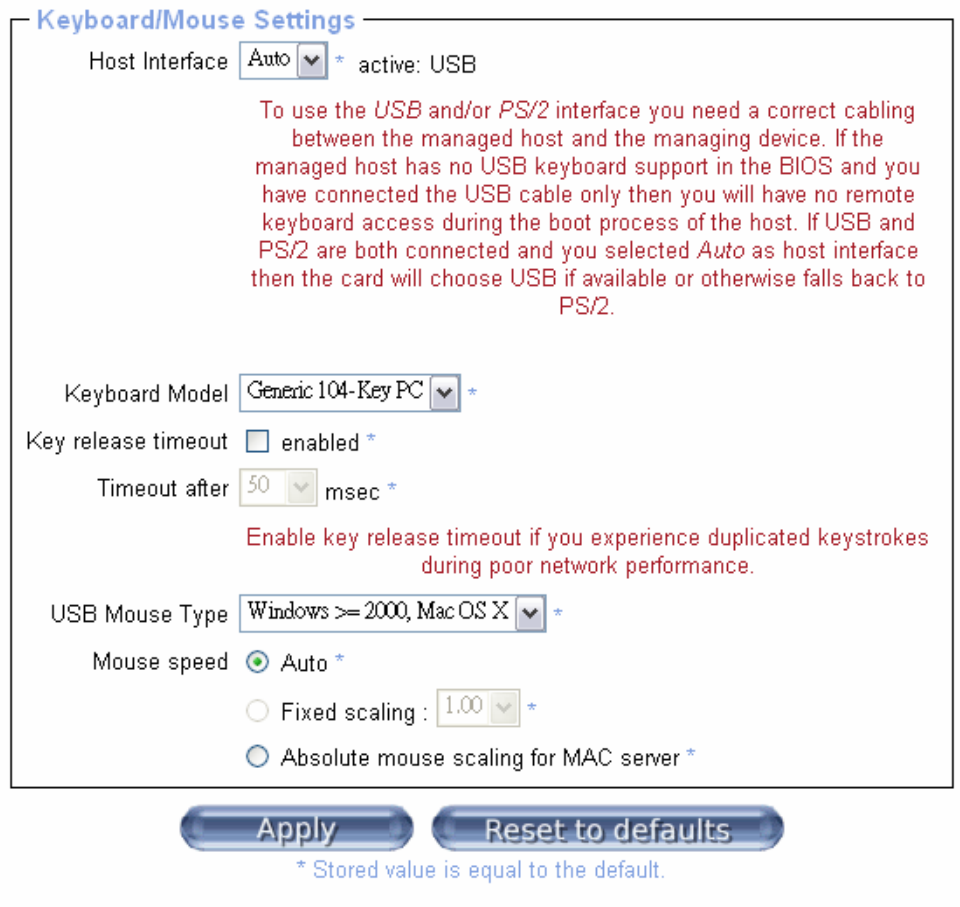

Keyboard/Mouse Settings
Host Interface
Auto
active: USB
To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected Auto as host interface then the card will choose USB if available or otherwise falls back to PS/2.
Keyboard Model
Generic 104-Key PC
Key release timeout
enabled
Timeout after
50
msec
Enable key release timeout if you experience duplicated keystrokes during poor network performance.
USB Mouse Type
Windows >= 2000, Mac OS X
Mouse speed
Auto
Fixed scaling :
1.00
Absolute mouse scaling for MAC server
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 5-16 Keyboard and Mouse Settings

Host Interface

Enables a certain interface the mouse is connected to. You can choose between “Auto” for automatic detection, “USB” for an USB mouse, and “PS/2” for a PS/2 mouse.

Warning

To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected “Auto” as host interface, then the card will select “USB” if available or otherwise falls back to “PS/2”.

To get USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

- the host BIOS must have USB keyboard support

- the USB cable must be connected or must be selected in the Host interface option

PS/2 Keyboard Model

Enables a certain keyboard layout. You can choose between “Generic 101-Key PC” for a standard keyboard layout, “Generic 104-Key PC” for a standard keyboard layout extendend by three additional windows keys, “Generic 106-Key PC” for a japanese keyboard, and “Apple Macintosh” for the Apple Macintosh.

Keyboard timeout

Recommanded as “enable” for keyboard timeout when host is UNIX or UNIX-like OS.

USB Mouse Type

Enables USB mouse type. Choose between “Windows >= 2000 , MacOSX” for MS Windows 2000 or Windows XP, Mac OSX or “Other Operating Systems” for MS Windows NT, Unix or Unix-like OS, or OS X. In “Windows >= 2000 , MacOSX” mode the remote mouse is always synchronized with the local mouse.

Mouse Speed

- Auto mouse speed

  Use this option if the mouse settings on host use an additional acceleration setting. The IP-101 tries to detect the acceleration and speed of the mouse during the mouse sync process.

- Fixed mouse speed

  Use a direct translation of mouse movements between the local and the remote pointer.

  You may also set a fixed scaling which determines the pixel-amount of the remote mouse pointer movement when the local mouse pointer is moved by one pixel. This option is used to manually control the remote mouse speed and only works when the mouse settings on the host are linear. This means mouse acceleration of OS should be disabled, and the intelligent mouse synchronization of IP-101 is not functioning under this setting.

- Absolute mouse scaling for MAC server

  Use this option for MAC server.

To set the options, click on the button **Apply**.

5.4.3 Video

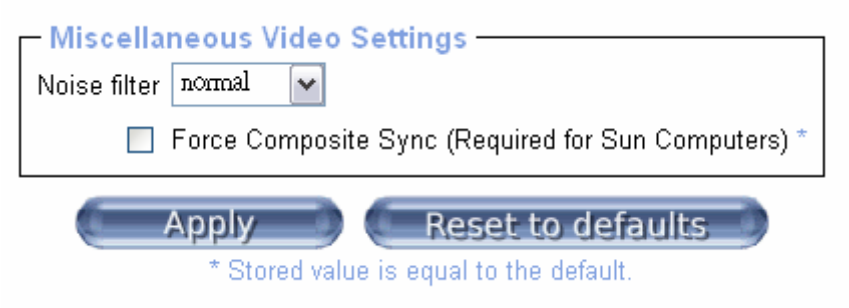


Figure 5-17 Video Settings

Miscellaneous Video Settings

- **Noise filter**

  This option defines how the IP-101 reacts to small changes in the video input signal. Turning on the noise filter can help reduce video flickering that is often caused by distortions, as well as lowering unnecessary bandwidth consumption. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

- **Force Composite Sync (Required for Sun Computers)**

  When connecting the device directly to legacy Sun computer (with composite sync as the video output, it may be possible that IP-101 don't recognize the composite sync automatically. To support signal transmission from a Sun machine, enable this option. If not enabled the picture of the remote console will not be visible.

To set the options, click on the button **Apply**.

5.5 Device Settings

5.5.1 Network

The Network Settings panel allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

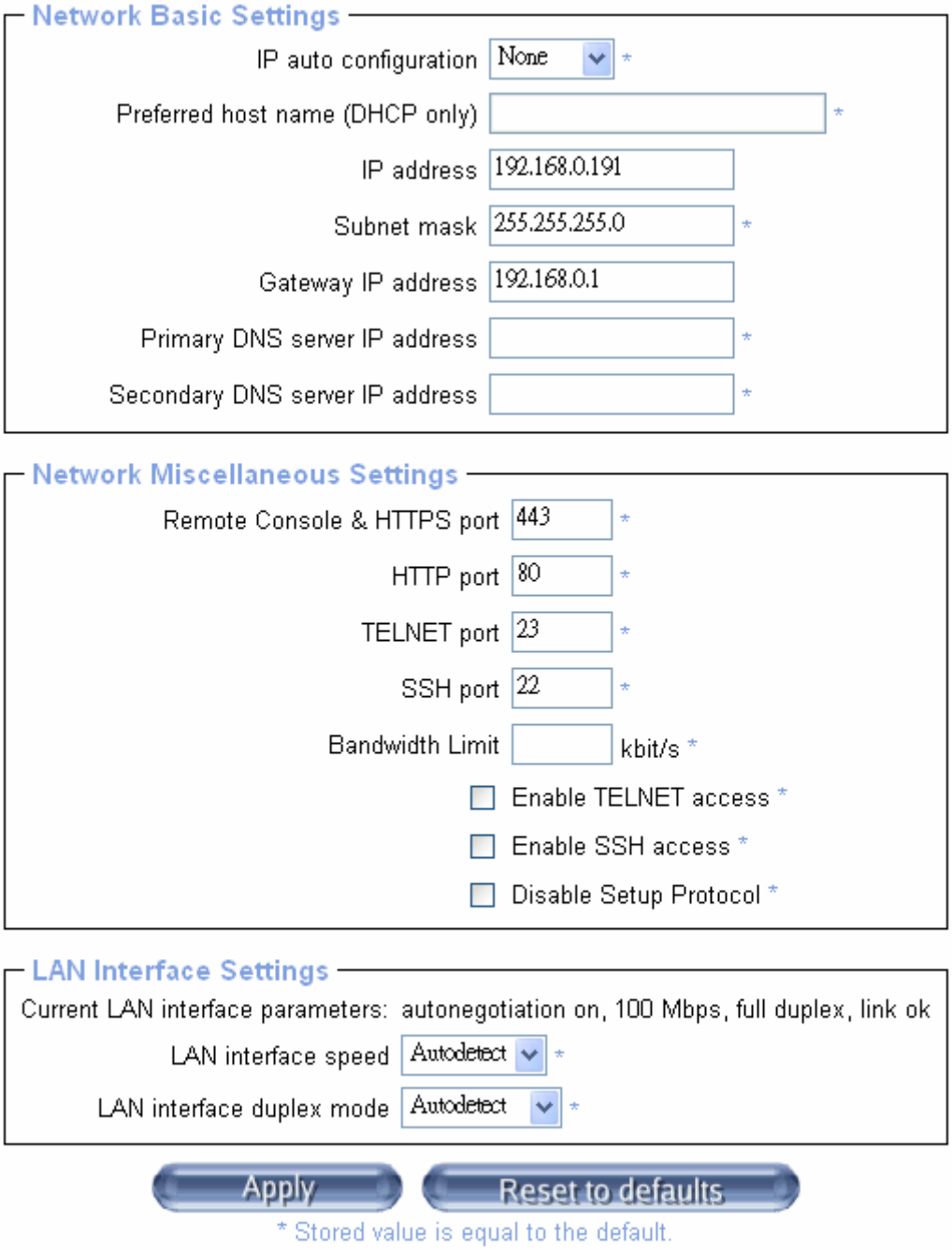


Figure 5-18 Netw ork Settings

Warning

Changing the network setting s of the IP-101 m ight result in losing co nnection to it. In case you change th e settings remotely make sure that all the values are correct and you still have an option to access the IP-101.

IP auto configuration

With this option you can control if the IP-101 should fetch its network settings from a DHCP or BOOTP server. For DHCP, select “dhcp” , and for BOOTP select “bootp” accordingly. If you choose “none” then IP auto configuration is disabled.

Preferred host name

Preferred host name to request from DHCP server. Whether the DHCP server takes the IP-101 suggestion into account or not depends on the server configuration.

IP address

IP address in the usual dot notation.

Subnet Mask

The net mask of the local network.

Gateway IP address

In case the IP-101 should be accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

Primary DNS Server IP Address

IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the IP-101 will not be able to perform name resolution.

Secondary DNS Server IP Address

IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

Remote Console And HTTPS port

Port number at which the IP-101's Remote Console server and HTTPS server are listening. If left empty the default value will be used.

HTTP port

Port number at which the IP-101's HTTP server is listening. If left empty the default value will be used.

Telnet port

Port number at which the IP-101's Telnet server is listening. If left empty the default value will be used.

SSH port

Port number at which the IP-101 SSH (Secure SHell) server is listening to. If left empty the default value (port 22) will be used.

Bandwidth limitation

The maximum network traffic generated through the IP-101 ethernet device. Value in Kbit/s.

Enable Telnet access

This enables the Telnet function.

Enable SSH access

This enables the SSH (Secure SHell) function.

Disable Setup Protocol

Enable this option to exclude the IP-101 from the setup protocol. Setup protocol is a proprietary layer-2 MAC-based protocol to allow some configuration software to detect IP-101 devices in the network, even without IP address, and then config network related settings to IP-101.

LAN Interface Settings

The "Autodetect" will set the ethernet speed to the fastest possible value supported by both endpoints of the link. For example, if you use a 10M/half duplex HUB, this speed will be auto-selected. If this option does not work with some network device (HUB, switches, and routers), you can set the Ethernet interface speed of IP-101 manually to the values as supported by the network device.

5.5.2 Dynamic DNS

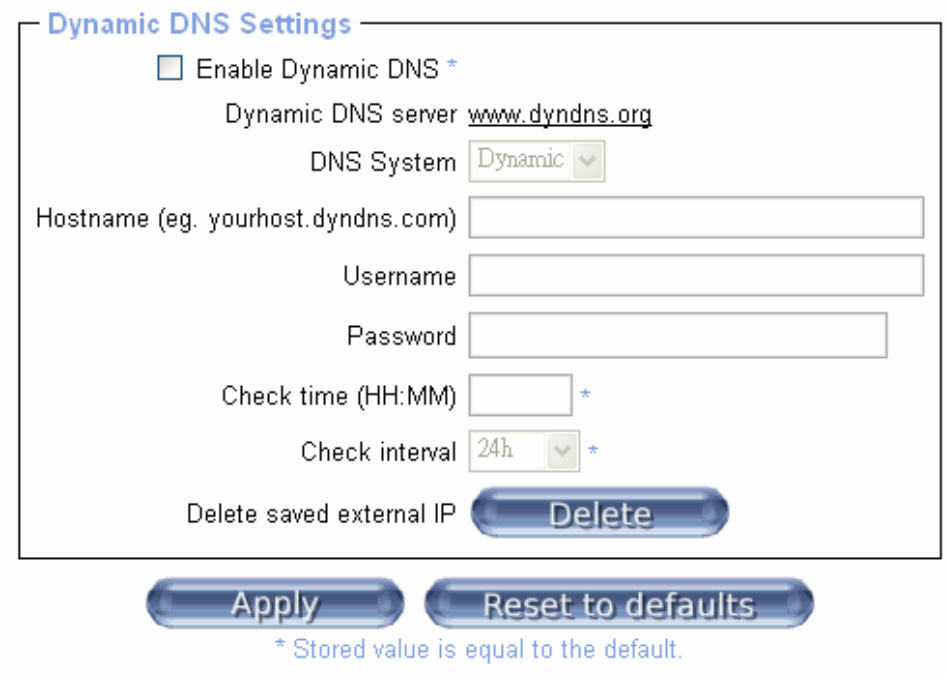


Figure 5-19 Dynamic DNS

A freely available Dynamic DNS service (www.dyndns.org) can be used in the following scenario.

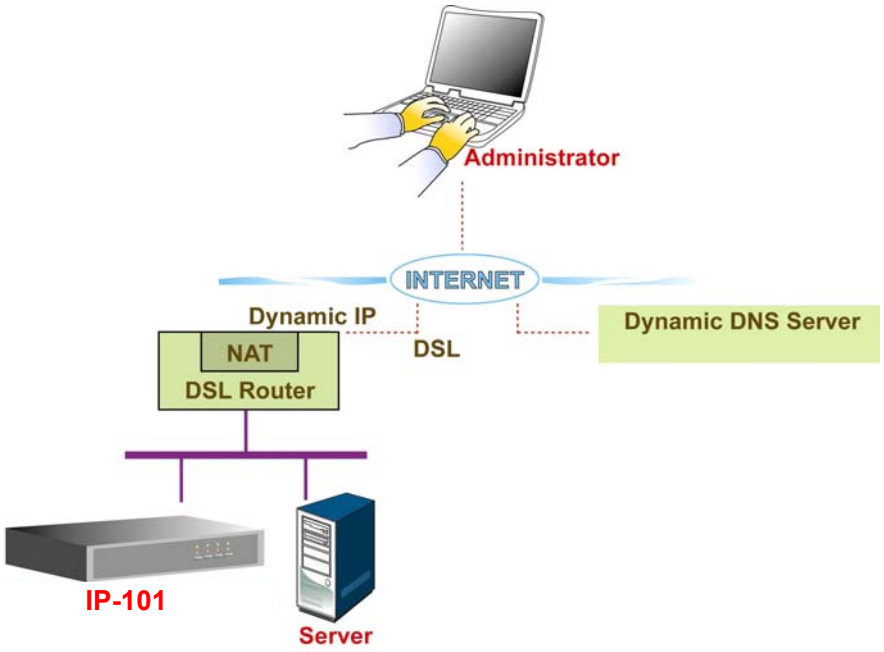


Figure 5-20 Dynamic DNS Scenario

The IP-101 is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the IP-101 connects to a special dynamic DNS server in regular intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to his card.

The administrator has to register an IP-101 that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nickname and a password in return to the registration process. This account information together with the hostname is needed in order to determine the IP address of the registered IP-101.

You have to perform the following steps in order to enable Dynamic DNS:

- Make sure that the LAN interface of the IP-101 is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in Figure.
- Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS

This enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server

This is the server name where IP-101 registers itself in regular intervals. Currently, this is a fixed setting since only dyndns.org is supported for now.

DNS System

Choose Dynamic for free DNS service. Custom for your own domain.

Hostname

This is the hostname of the IP-101 that is provided by the Dynamic DNS Server. (use the whole name including the domain, e.g. testserver.dyndns.org , not just the actual hostname).

Username

You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password

You have used this password during your manual registration with the Dynamic DNS Server.

Check time

The IP-101 registers itself for initiating the IP address of IP-101 stored in the Dynamic DNS server at this time.

Check interval

This is the interval for reporting again to the Dynamic DNS server for updating the IP address associated with the Domain Name of the IP-101.

Warning

The IP-101 has its own independent real time clock. Make sure the time setting of the IP-101 is correct. (see the Section *Date And Time*)

5.5.3 Security

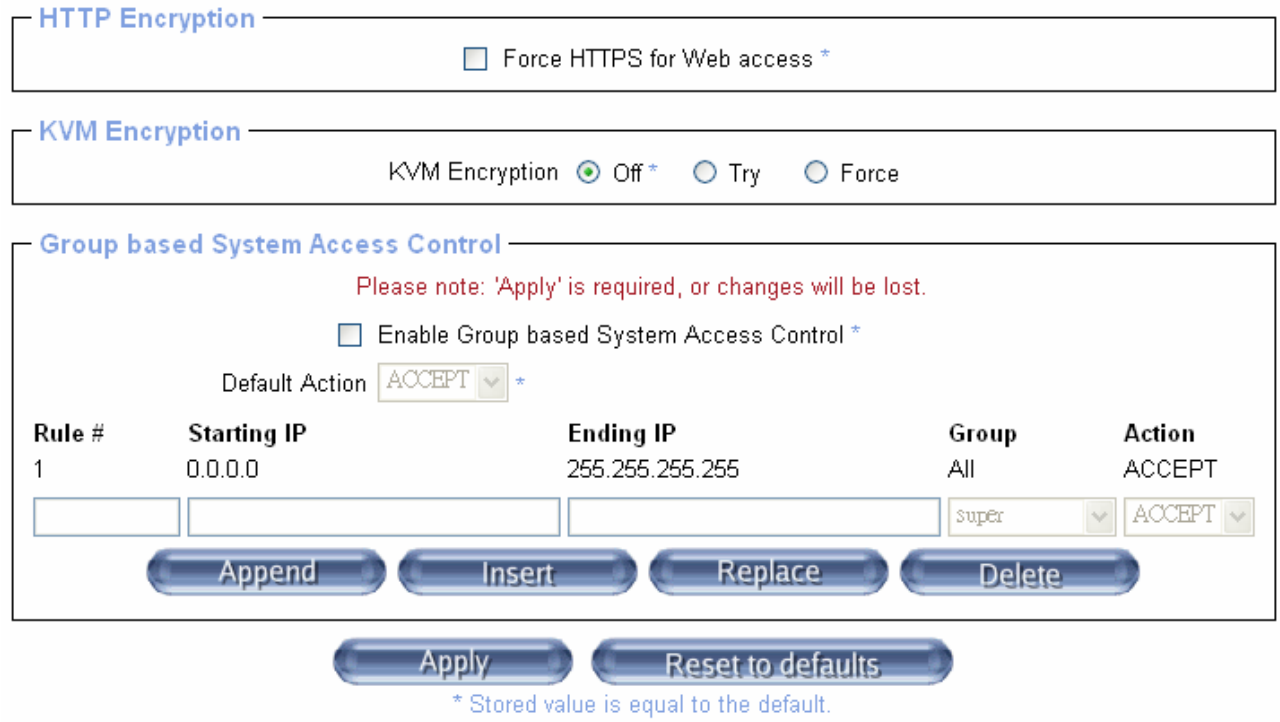

HTTP Encryption
Force HTTPS for Web access *
KVM Encryption
KVM Encryption Off * Try Force
Group based System Access Control
Please note: 'Apply' is required, or changes will be lost.
Enable Group based System Access Control *
Default Action ACCEPT *
Rule # Starting IP Ending IP Group Action
1 0.0.0.0 255.255.255.255 All ACCEPT
super ACCEPT
Append Insert Replace Delete
Apply Reset to defaults
* Stored value is equal to the default.

Figure 5-21 Device Security

Force HTTPS

If this option is enabled access to the web front-end is only possible using an HTTPS connection. The IP-101 will not listen on the HTTP port for incoming connections.

In case you want to create your own SSL certificate that is used to identify the IP-101 refer to the Section called *Certificate*.

KVM encryption

This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host. If set to “Off” no encryption will be used. If set to ”Try” the applet tries to make an encrypted connection. In case connection establishment fails for any reason an unencrypted connection will be used.

If set to “Force” the applet tries to make an encrypted connection with certificate. An error will be reported in case connection establishment fails.

Group-based System Access Control

This is the IP filtering function, it keeps unauthorized hosts from accessing to the IP-101 by specifying IP filtering rules. It is important to fully understand what an IP filter is. If you don't fully understand this, you will get unexpected results against your original plan.

Chain rule

The **Chain rule** determines whether the access from the hosts is allowed or not. It can be one of these two values:

- ACCEPT : access allowed
- DROP : access not allowed

The rule can be configured to apply to a particular Group level (All, User, Super, Administrator).

When the IP-101 receives a TCP packet, it will process the packet with the chain rule depicted below. The process ordering is important; The packet will enter the chain rule 1 first, if meet the rule then take action directly, otherwise go to chain rule 2.

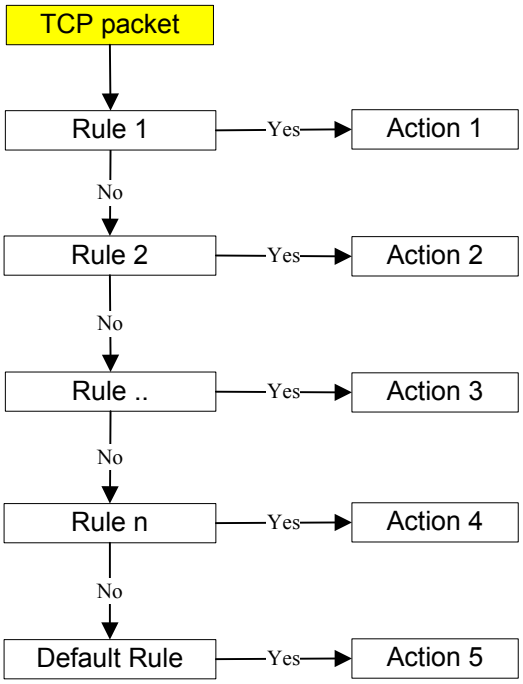
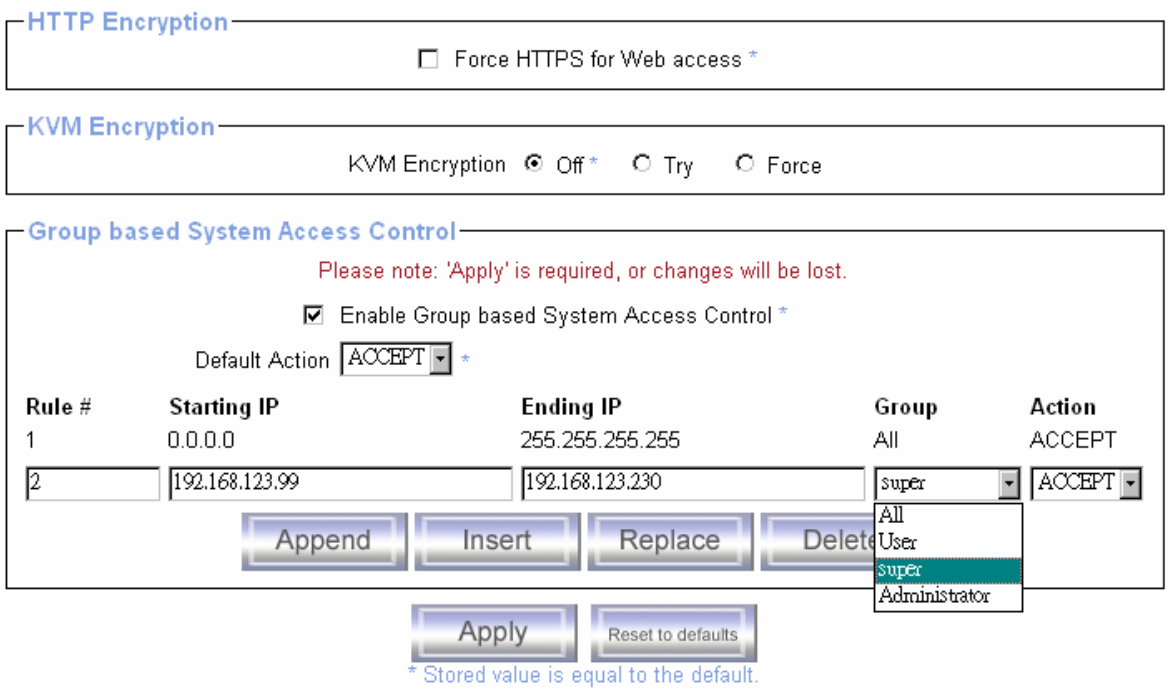
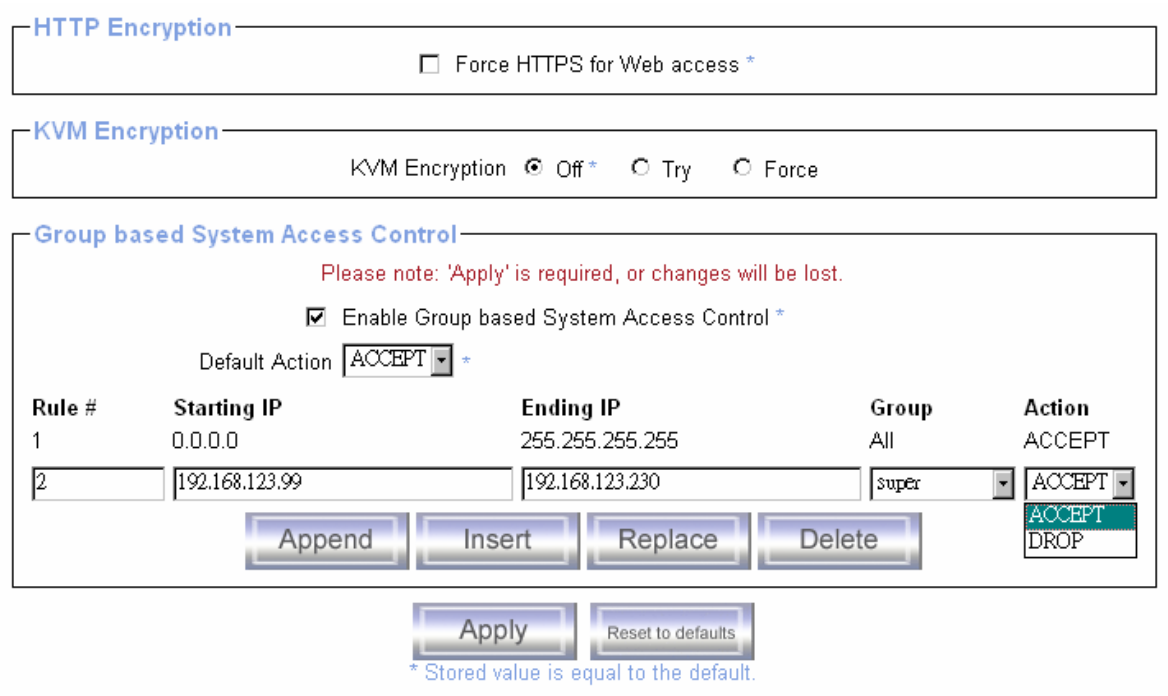


Figure 5-22 Chain Rules of IP Filtering

Check the “Enable Group based System Access Control” to edit the rules

Users can add a new IP filtering rule by setting the properties at adding line by **Append** or **Insert**. User can remove a rule by **Remove** or **Delete**.


HTTP Encryption
Force HTTPS for Web access *
KVM Encryption
KVM Encryption Off * Try Force
Group based System Access Control
Please note: 'Apply' is required, or changes will be lost.
Enable Group based System Access Control *
Default Action ACCEPT *
Rule # Starting IP Ending IP Group Action
1 0.0.0.0 255.255.255.255 All ACCEPT
2 192.168.123.99 192.168.123.230 super ACCEPT
All
User
Super
Administrator
Append Insert Replace Delete
Apply Reset to defaults
* Stored value is equal to the default.


HTTP Encryption
Force HTTPS for Web access *
KVM Encryption
KVM Encryption Off * Try Force
Group based System Access Control
Please note: 'Apply' is required, or changes will be lost.
Enable Group based System Access Control *
Default Action ACCEPT *
Rule # Starting IP Ending IP Group Action
1 0.0.0.0 255.255.255.255 All ACCEPT
2 192.168.123.99 192.168.123.230 super ACCEPT
ACCEPT
DROP
Append Insert Replace Delete
Apply Reset to defaults
* Stored value is equal to the default.

5.5.4 Certificate

Figure 5-23 Certificate Settings

The IP-101 uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the IP-101 has to expose its identity to a client using a cryptographic certificate. The default certificate comes with IP-101 device upon delivery is for testing purpose only. System administrator should not rely on this default certificate as the secured global access mechanism through Internet.

However, it is possible to generate and install a new base64 X.509 certificate that is unique for a particular IP-101 In order to do that, the IP-101 is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are, and signs and issues a SSL certificate to you.

The following steps are necessary to create and install a SSL certificate for the IP-101:

- Create a SSL Certificate Signing Request using the panel shown in Figure. You need to fill out a number of fields that are explained below. Once this is done, click on the button “Create” which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the “Download CSR” button.

- Send the saved CSR string to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).
- Upload the certificate to the IP-101 using the “Upload” button as shown in Figure below.

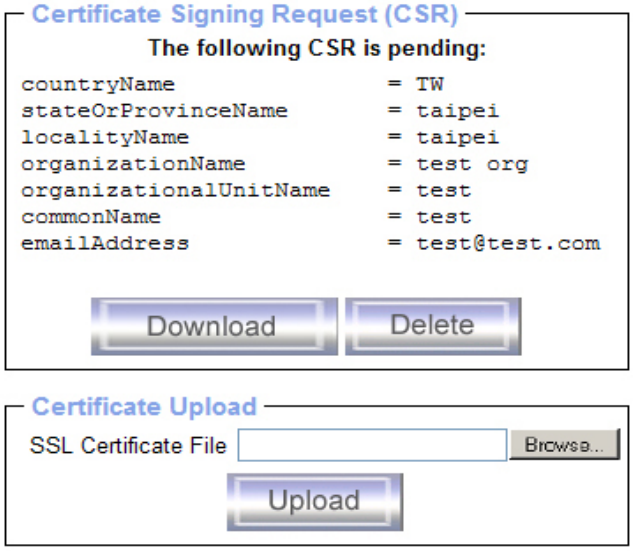


Figure 5-24 SSL Certificate Upload

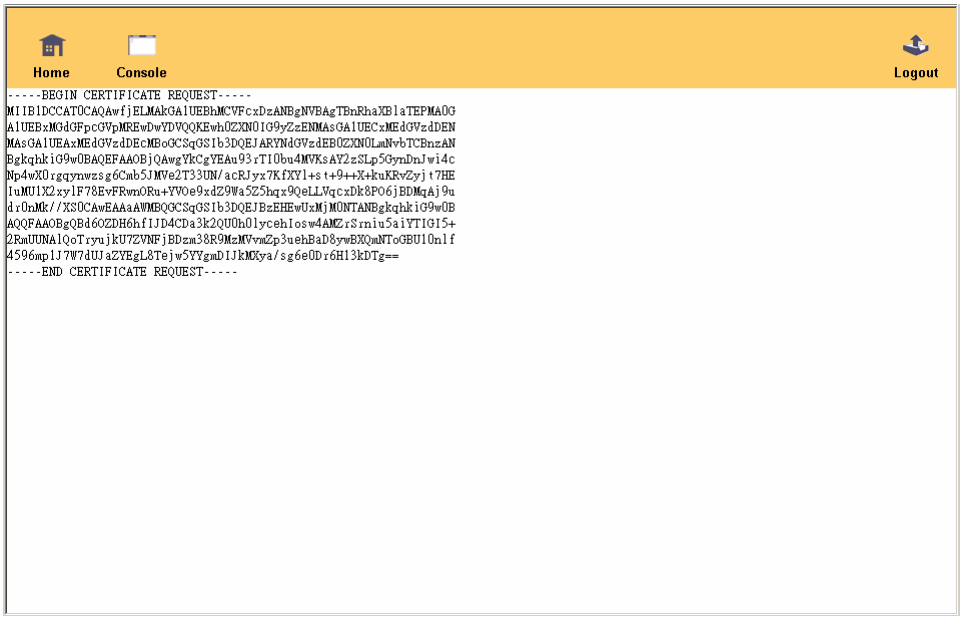


Figure 5-25 CSR string

After completing these three steps, the IP-101 has its own certificate that is used for identifying the card to its clients.

> **Warning**
>
> If you destroy the CSR on the IP-101 there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above.

Common name

This is the network name of the IP-101 once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the IP-101 with a web browser (without the “http://” prefix). In case the name given here and the actual network name differ, the browser will pop up a security warning when the IP-101 is accessed using HTTPS.

Organizational unit

This field is used for specifying to which department within an organization the IP-101 belongs.

Organization

The name of the organization to which the IP-101 belongs.

Locality /City

The city where the organization is located.

State/P rovince

The state or province where the organization is located.

Country (ISO code)

The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the USA. (Note: the country code has to be entered in CAPITAL LETTERS.)

Challenge Password

Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is 4 characters.

Confirm Challenge Password

Confirmation of the Challenge Password

Em ail

The email address of a contact person that is responsible for the IP-101 and its security.

Key length

This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the IP-101 during connection establishment.

5.5.5 Serial Port

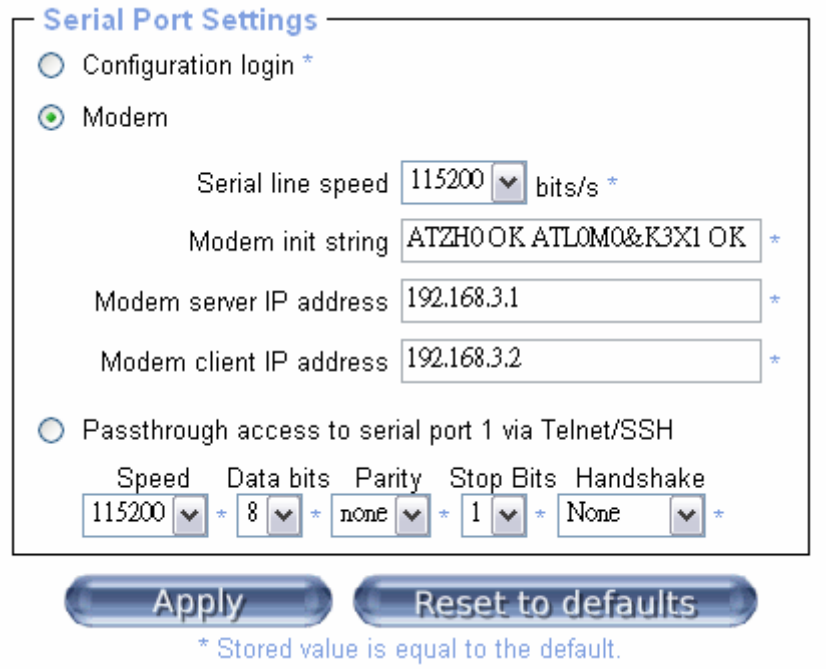

Serial Port Settings
Configuration login *
Modem
Serial line speed 115200 bits/s *
Modem init string ATZH0 OK ATL0M0&K3X1 OK *
Modem server IP address 192.168.3.1 *
Modem client IP address 192.168.3.2 *
Passthrough access to serial port 1 via Telnet/SSH
Speed Data bits Parity Stop Bits Handshake
115200 * 8 * none * 1 * None *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 5-26 Serial Port

The IP-101 Serial Settings allows you to specify what device is connected to the serial port and how to use it.

Configuration or console login

Do not use the serial port for any special function, use it only for the initial configuration.

Modem

The IP-101 offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the serial interface of the IP-101 .

Logically, connecting to the IP-101 using a telephone line means nothing else than building up a dedicated point-to-point connection from your console computer to the IP-101. In other words, the IP-101 acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the IP-101, make sure to configure your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection, which defaults to the right settings like PPP.

The Modem Settings panel allows you to configure the remote access to the IP-101 using a modem. The meaning of each parameter will be described below. The modem settings are part of the serial settings panel.

5.5.4 Certificate

Figure 5-23 Certificate Settings

The IP-101 uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the IP-101 has to expose its identity to a client using a cryptographic certificate. The default certificate comes with IP-101 device upon delivery is for testing purpose only. System administrator should not rely on this default certificate as the secured global access mechanism through Internet.

However, it is possible to generate and install a new base64 X.509 certificate that is unique for a particular IP-101 In order to do that, the IP-101 is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are, and signs and issues a SSL certificate to you.

The following steps are necessary to create and install a SSL certificate for the IP-101:

- Create a SSL Certificate Signing Request using the panel shown in Figure. You need to fill out a number of fields that are explained below. Once this is done, click on the button “Create” which will ini itiate the Certificate S igning Request generation. The CSR can be downloaded to your administration machine with the “Download CSR” button.

5.5.6 Date / Time

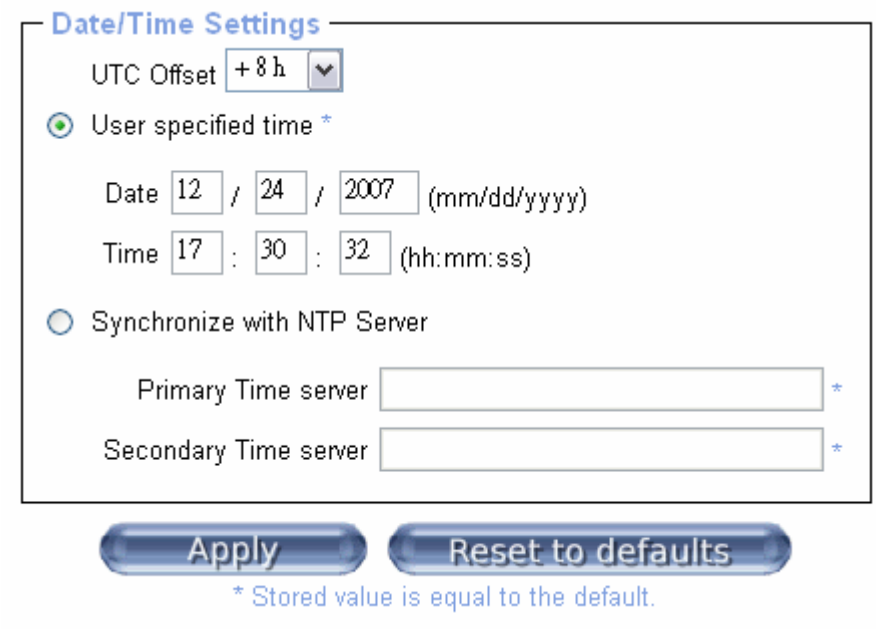

Date/Time Settings
UTC Offset +8 h
User specified time *
Date 12 / 24 / 2007 (mm/dd/yyyy)
Time 17 : 30 : 32 (hh:mm:ss)
Synchronize with NTP Server
Primary Time server *
Secondary Time server *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 5-27 Date / Time

This link refers to a page, where the internal real-time clock of the IP-101 can be set up. You have the possibility to adjust the clock manually, or to use a NTP timeserver. Without a timeserver, your time setting will not be persistent, so you have to adjust it again, after IP-101 loses power for more than a few minutes. To avoid this, you can use a NTP timeserver, which sets up the internal clock automatically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

Warning

There is cur rently no w ay to adjust the dayligh t saving time autom atically. So you have to set up the UTC offset twice a year properly to the local rules of your country.

5.5.7 Event Log

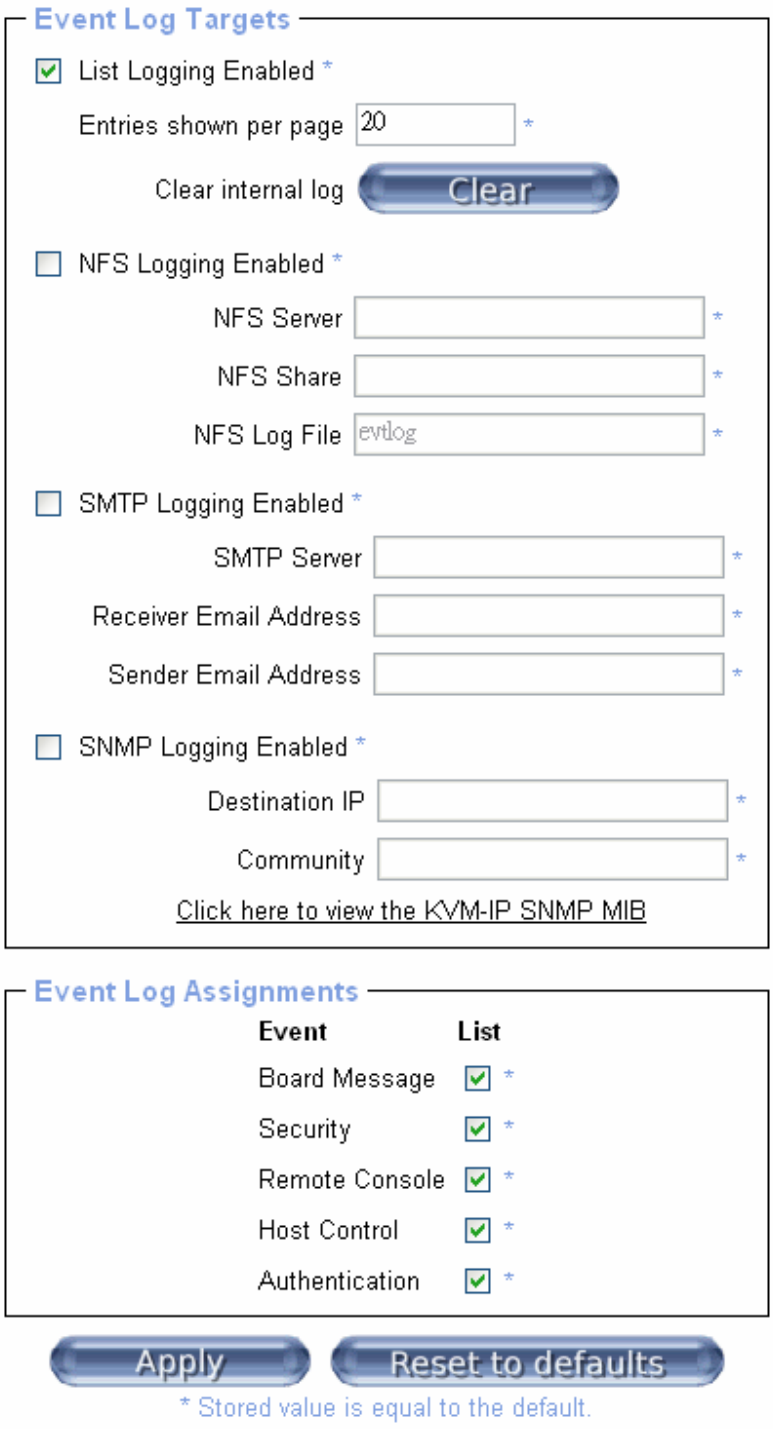


Figure 5-28 Event Log

Important events like a login failure or a firmware update are logged to a selection of logging destinations. Each of those events belongs to an event group, which can be activated separately.

The common way to log events is to use the internal log list of the IP-101. To show the log list, click on “Event Log” on the “Maintenance” page. In the Event Log Settings you can

choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

List logging enabled

The common way to log events is to use the internal log list of the IP-101. To show the log list, click on “Event Log” on the “Maintenance” page.

Since the IP-101's system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1,000 events. Every entry that exceeds this limit overrides the oldest one, automatically.

> **Warning**
>
> If the reset button on the HTML frontend is used to restart the IP-101, all logging information is saved permanently and is available after the IP-101 has been started. If the IP-101 loses power or a hard reset is performed, all logging data will be lost. To avoid this, use one of the following log methods.

NFS Logging enabled

Define a NFS server, where a directory or a static link have to be exported, to write all logging data to a file that is located there. To write logging data from more than one IP-101 devices to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the button “Apply” , the NFS share will be mounted immediately. That means, the NFS share and the NFS server must be filled with valid sources or you will get an error message.

SMTP Logging enabled

With this option, the IP-101 is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server, that has to be reachable from the IP-101 device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

If this is activated, the IP-101 sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have an own trap class that consists of several fields with detailed information about the occurred event. To receive this SNMP traps, any SNMP trap listener may be used.

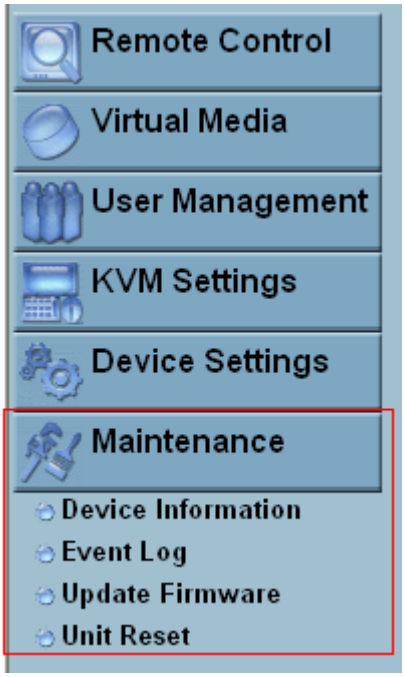
Here is a example of all gerenated event and its event group.

Device succesfully started	device
Board Reset performed by user...	device
Firmware upload failed.	device
No firmware file uploaded.	device
Uploaded firmware file discarded.	device
Firmware validation failed.	device
Firmware file uploaded by user...	device
Firmware updated by user...	device
Internal log file cleared by user...	device
Security Violation	security
Host Power	host
Host Reset	host
Connection to Remote Console failed: reason.	console (several)
Connection to client ... established.	console
Connection to client ... closed.	console
Login failed.	auth
Login succeed.	auth

Warning

In contrast to the internal log file on the IP-101, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete it or move it away from time to time.

5.6 Maintenance



5.6.1 Device Information

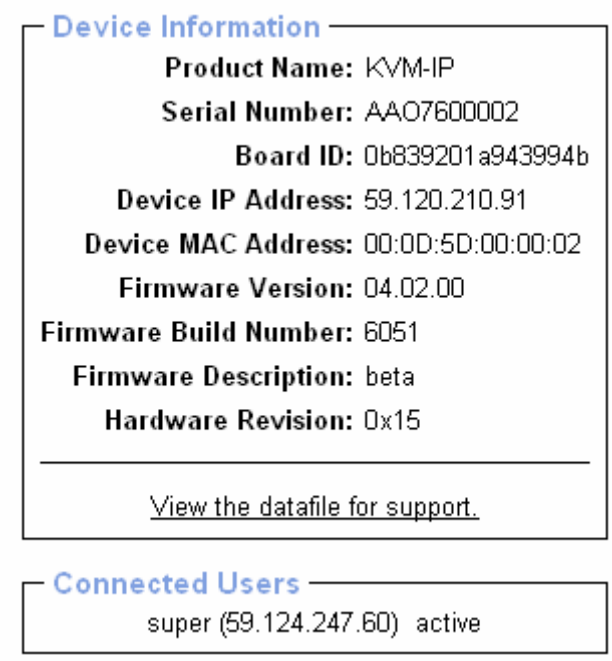


Figure 5-29 Device Information

Device Summary

This section contains a summary with various information about this IP-101 and it's current firmware and allows you to reset the card.

The Data file for support allows you to download the IP-101 data file with specific support information. This is an XML file with certain customized support information like the serial

number etc. You may send us this information together with a support request. It will help us to locate and solve your reported problem.

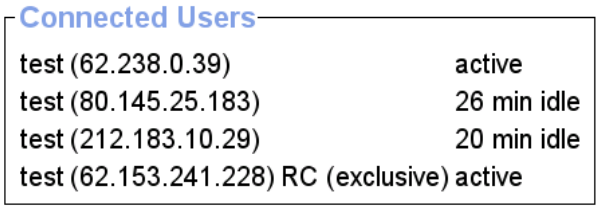

Connected Users
test (62.238.0.39) active
test (80.145.25.183) 26 min idle
test (212.183.10.29) 20 min idle
test (62.153.241.228) RC (exclusive) active

Figure 5-30 Connected Users

Figure above displays the IP-101 activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. RC means that the Remote Console is open. If the Remote Console is opened in exclusive mode the term (exclusive mode) is added. For more information about this option see the Section called Remote Console Control Bar.
To display the user activity the last column contains either the term active for an active user or 30 min idle for an user who is inactive for a certain amount of time.

5.6.2 Even log

Event Log

[Prev][Next]

Date	Event	Description
10/12/2007 07:26:07	Authentication	User 'super' logged in from IP address 220.135.171.106
10/12/2007 00:07:54	Remote Console	Connection to client 59.120.210.87 closed.
10/12/2007 00:06:19	Remote Console	Connection to client 59.120.210.87 established.
10/12/2007 00:05:57	Authentication	User 'super' logged in from IP address 59.120.210.87
10/12/2007 00:05:41	Remote Console	Connection to client 59.120.210.87 closed.
10/12/2007 00:05:20	Remote Console	Connection to client 59.120.210.87 established.
10/12/2007 00:04:39	Authentication	User 'demo' logged in from IP address 59.120.210.87
10/11/2007 10:22:00	Remote Console	Connection to client 220.135.171.106 closed.
10/11/2007 10:17:11	Remote Console	Connection to client 220.135.171.106 established.
10/11/2007 10:16:46	Authentication	User 'demo' logged in from IP address 220.135.171.106
10/11/2007 08:31:28	Remote Console	Connection to client 60.250.63.98 closed.
10/11/2007 08:30:15	Remote Console	Connection to client 60.250.63.98 established.
10/11/2007 08:29:56	Authentication	User 'super' logged in from IP address 60.250.63.98
10/11/2007 08:29:16	Authentication	User 'super' logged in from IP address 60.250.63.98
10/11/2007 07:06:54	Remote Console	Connection to client 60.250.63.98 closed.
10/11/2007 07:00:15	Remote Console	Connection to client 60.250.63.98 established.
10/11/2007 07:00:02	Authentication	User 'super' logged in from IP address 60.250.63.98
10/11/2007 06:59:30	Remote Console	Connection to client 60.250.63.98 closed.
10/11/2007 06:55:26	Remote Console	Connection to client 60.250.63.98 established.
10/11/2007 06:55:20	Remote Console	Connection to client 60.250.63.98 closed.

[Prev][Next]

Figure 5-31 Event Log List

The figure above displays the log list including the events that are logged by the IP-101

5.6.3 Update Firmware

Figure 5-32 Update Firmware

The IP-101 is a complete standalone computer. The software it runs is called firmware. The firmware of the IP-101 can be updated remotely in order to install new functionality or special features.

A new firmware update is a binary file which will be sent to you by email or which you can download from the supplier web site. If the firmware file is compressed (file suffix .zip) then you must unzip it before you can proceed. Under the Windows operating system you may use WinZip from http://www.winzip.com/ for decompression. Other operating systems might provide a program called unzip.

Before you can start updating the firmware of your IP-101 the new uncompressed firmware file has to be accessible on the system that you use for connecting to the IP-101.

Updating the firmware is a three-stage process:

- Firstly, the new firmware file is uploaded onto the IP-101. In order to do that you need to select the file on your local system using the button “Browse” of the Upload Firmware panel. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted.
- Secondly, if everything went well, you see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the button “Update” will store the new version and substitute the old one completely.

Warning

This process is not reversible and might take some minutes. Make sure the IP-101's power supply will not be interrupted during the update process, because this may cause an unusable card.

- Thirdly, after the firmware has been stored, the panel will request you to reset the IP-101 manually. Half a minute after the reset, the IP-101 will run with the new firmware version and should be accessible. However, you are requested to login once again.

Warning

The three-stage firmware update process and complete consistency check are making a mistake in updating the firmware almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure the IP-101's power supply will not be interrupted!

5.6.4 Unit Reset

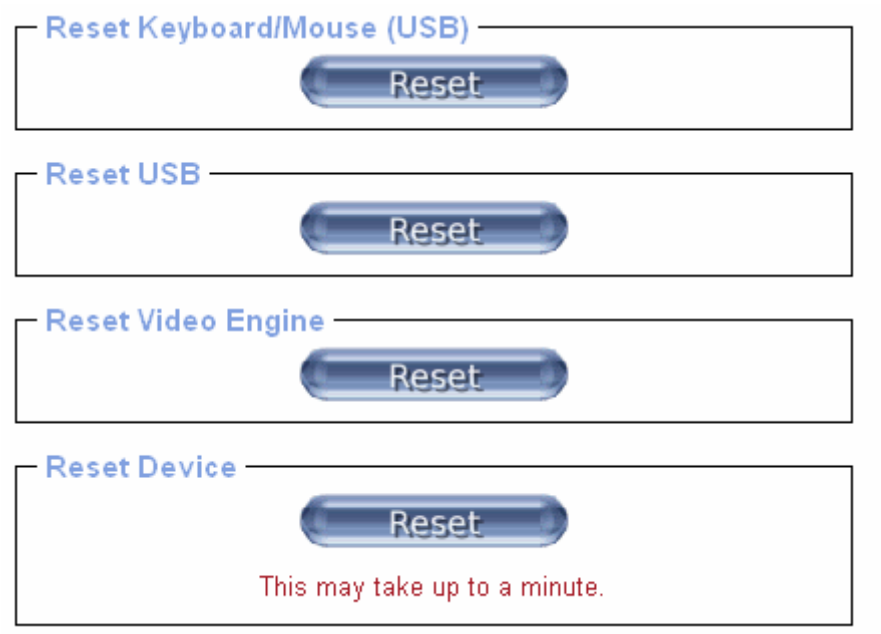


Figure 5-33 Unit Reset

This section allows you to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the IP-101 itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console.

The whole process will take about half a minute. Resetting sub devices (e.g. video engine) will take some seconds only and does not result in closing connections. To reset a certain IP-101 functionality click on the button Reset.

Note: Only the super user is allowed to reset the IP-101.

6. Technical Specifications

Model No.	**IP - 101**
Target Device Connection	1 x Keyboard PS/2 Mini Din 6 Pin 1 x Mouse PS/2 Mini Din 6 Pin 1 x VGA HD-15 1 x USB 2.0 Type A receptacle
Local Access Connection	1 x PS/2 Keyboard Mini Din 6 Pin 1 x PS/2 Mouse Mini Din 6 Pin 1 x VGA HD-15
Remote Access Connection	1 x RJ-45
Network Connection	10/100 Ethernet, telephone line (modem needed)
Firmware Upgrade Port	1 x Serial DB9 Pin
Max. Video Resolution	Local- 1600 x 1200 Remote- 1280 x 1024
OS Compatibility	MS Windows family, Unix, Sum Solaris, Linux, Mac OSX
Browser Compatibility	IE 6.0, Netscape 7.0, Mozilla 1.6 (or above)
IP Setting	DHCP, Bootp, Fixed IP (DDNS supported)
Management Interface	Web, Utility, Telnet, Serial port
Event Log	NFS, SMTP, SNMP trap
Housing Material	Metal
Power adaptor	input- 12V/1.25A
Operating Temperature	0-50℃
Storage Temperature	-20 – 60℃
Weight (gram)	485 g
Size (mm)	110(L) x 121(W) x 41(H)

7. Troubleshooting

1. **The remote mouse doesn't work or is not synchronous**
   Make sure the mouse settings in IP-101 match the mouse model. There are some circumstances where the mouse synchronization process could behave incorrectly, refer to Sections 5.4.1 & 6.5.22 for further explanation.

2. **The video quality is bad or the picture is grainy**
   Try to correct the brightness and contrast settings (see Sections 5.4.1 & 6.5.3) until they are out of a range where the picture looks grainy. Use the auto adjustment feature to correct a flickering video.

3. **Login on IP-101 fails.**
   Was the correct combination of user and password given? On delivery, the user "super" has the password "pass". Moreover your browser must be configured to accept cookies.

4. **The Remote Console window can't connect to IP-101**.
   Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connection establishments.

5. **No connection can be established to IP-101.**
   Check whether the network connection is working in general (ping the IP address of IP-101). If not, check network hardware. Is IP-101 powered on? Check whether the IP address of IP-101 and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, like routers etc., is correctly configured. Without a ping functioning, IP-101 can't work either.

6. **Special key combinations, e.g. ALT+F2, ALT+F3 are intercepted by the console system and not transmitted to the host.**
   You have to define a so-called 'Button Key'. This can be done in the Remote Console settings.

7. **In the browser the IP-101 pages are inconsistent or chaotic.**
   Make sure your browser cache settings are feasible. Especially make sure the cache settings are not set to something like "never check for newer pages". Otherwise IP-101 pages may be loaded from your browser cache and not from the card.

8. **Windows XP doesn't awake from standby mode**
   This is possibly a Windows XP problem. Try not to move the mouse while XP goes in standby mode.

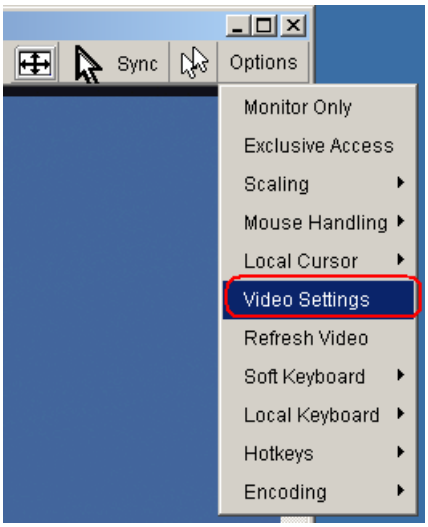
9. **Can't upload the signed certificate in MacOS X**
   If an 'internal error' occurs while uploading the signed certificate either change the

extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is plain text and the checkbox 'use for outgoing' is checked. Another possibility is to use a Mozilla based browser.

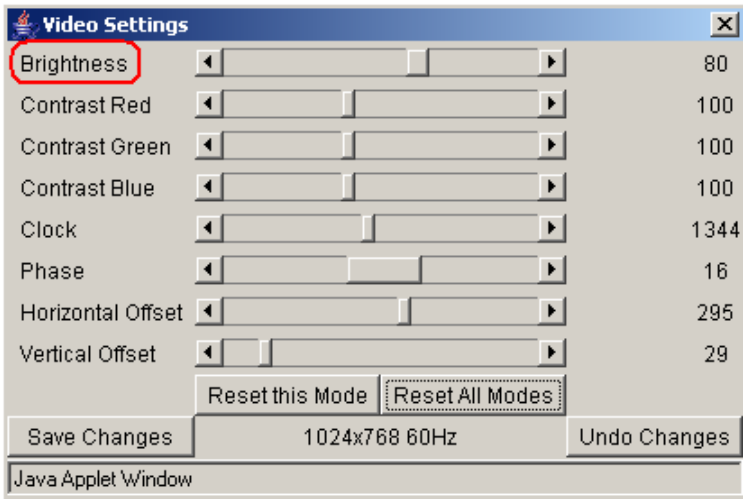
10. **Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore**
    Please check, if you have an option like "Automatically move mouse pointer to the default button of dialog boxes" enabled in the mouse settings of the operating system. This option needs to be disabled.

8. FAQs

1. **The color of remote console displaying a pinkish tint.**
   If you are experiencing the **remote control screen displaying a pinkish tint** with some graphic cards, please try adjusting the brightness of the remote console by following steps below.
   a) Click **Video Settings** in Options menu of the remote console.



   b) Adjust the **Brightness** setting until the pinkish tint is reduced or eliminated.



2. **Does any software require on servers which connect to the IP-101?**
   No, the IP-101 is a 100% hardware solution. No extra software require on servers.

3. **What operating systems does IP-101 support?**
   The IP-101 supports Windows 98, Windows ME, Windows 2000/XP and above, , Unix, Unix-like Operating System (Sun Solaris, Linux) and Mac OSX.

4. **What browsers does IP-101 support?**
   The IP-101 support Microsoft Internet Explorer version 6.0 or higher, Netscape 7.0 and

Mozilla 1.6.

5. **Does the IP-101 work with other brand's KVM switch?**
   Yes, the IP-101 can work with most standard KVM.

6. **How many letters the username and password can be set on IP-101?**
   The IP-101 accepts 32 letters of username and password.

7. **How many concurrent user of IP-101?**
   The IP-101 accepts 15 concurrent users.

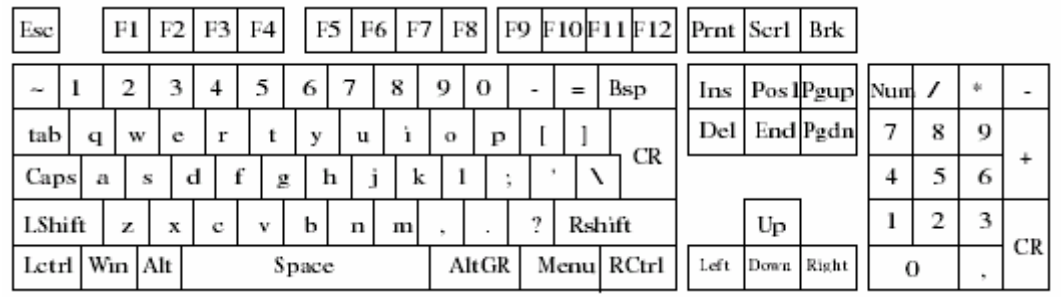
8. **How many bits of connection encrypted of IP-101?**
   The IP-101 provides AES 256 bits connection encrypted.

9. **Local mouse and remote mouse didn't sync after doing mouse Intelligent Sync.**
   Please don't put window on left-up corner of remote console of IP-101. Intelligent Sync has to re-calculate the coordinate of mouse from left-up corner on remote console.

9. Addendum

A. Key Codes

Table below shows the key codes used to defines keystrokes or hotkeys for several functions. Please note that these key codes do not represent necessarily key characters that are used on international keyboards. They name a key on a standard 104 key PC keyboard with an US English language mapping. The layout for this keyboard is shown in figure below. However, most modifier keys and other alphanumeric keys used for hotkey purposes in application programs are on an identical position, no matter what language mapping you are using. Some of the keys have aliases also, means they can be named by 2 key codes (separated by comma in the table).


Esc
F1 F2 F3 F4
F5 F6 F7 F8
F9 F10 F11 F12
Prnt Scrl Brk
~ 1 2 3 4 5 6 7 8 9 0 - = Bsp
Ins Pos1 Pgup
Num / * -
tab q w e r t y u i o p [ ] CR
Del End Pgdn
7 8 9 +
Caps a s d f g h j k l ; ' \
4 5 6
LShift z x c v b n m , . ? Rshift
Up
1 2 3 CR
Lctrl Win Alt Space AltGR Menu RCtrl
Left Down Right
0 .

Key (and aliases)		
0 - 9	SPACE	PAGE DOWN
A - Z	ALTGR	UP
, TILDE	ESCAPE, ESC	LEFT
-, MINUS	F1	DOWN
=, EQUALS	F2	RIGHT
;	F3	NUM LOCK
’	F4	NUMPAD0
<, LESS	F5	NUMPAD1
,	F6	NUMPAD2
.	F7	NUMPAD3
/, SLASH	F8	NUMPAD4
BACK SPACE	F9	NUMPAD5
TAB	F10	NUMPAD6
[	F11	NUMPAD7
]	F12	NUMPAD8
ENTER	PRINTSCREEN	NUMPAD9
CAPS LOCK	SCROLL LOCK	NUMPADPLUS,NUMPAD PLUS
\, BACK SLASH	BREAK	NUMPAD/
LSHIFT, SHIFT	INSERT	NUMPADMUL,NUMPAD MUL
RCTRL	HOME	NUMPADMINUS,NUMPAD MINUS
RSHIFT	PAGE UP	NUMPADENTER
LCTRL, CTRL	DELETE	WINDOWS
LALT, ALT	END	MENU

B. Video Modes

Table below lists the video modes IP-101 supports. Please don't use other custom video settings besides of these. If done so, IP-110 may not be able to detect them.

Resolution (x, y)	Refresh Rates (Hz)
640 x 350	70, 85
640 x 400	56, 70, 85
640 x 480	60, 72, 75, 85, 90, 100, 120
720 x 400	70, 85
800 x 600	56, 60, 70, 72, 75, 85, 90, 100
832 x 624	75
1024 x 768	60, 70, 72, 75, 85, 90, 100
1152 x 864	75
1152 x 870	75
1152 x 900	66
1280 x 960	60
1280 x 1024	60, 75
1600 x 1200	60

C. User Role Permissions

Table below lists the user role permissions granted for three user role groups: "Superuser", "Administrator", and "User"

Function User		Administrator	Superuser
Remote Control: KVM	x x		x
Remote Control: Remote Power	- x		x
Remote Control: Telnet Console	x x		x
Virtual Media	x x		x
User Management: Change Password	x x		x
User Management: Users	- -		x
KVM Settings: User Console	x (w/o Misc. Settings)	x x	
KVM Settings: Keyboard/Mouse	- x		x
KVM Settings: Video	- x		x
Device Settings	- -		x
Maintenance: Device Information	x x		x
Maintenance: Event Log	- -		x
Maintenance: Update Firmware	- -		x
Maintenance: Unit Reset	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video	Keyboard/ Mouse, Video, Device

D. IP-101 TCP port number

Port Prot	ocol	Purpose
23	Telnet over TCP	Web & Telnet client
80	HTTP over TCP	Web
443	HTTP over TCP	Web
443	RFB over TCP	Remote Console
443	HTTPS over TCP	Drive Redirection
139	SMB over TCP	CD-ROM Image (Samba Service)
139	SMB over TCP	Floppy disk(Samba Service)
1024	SMB over TCP	Samba Service source port
162	SNMP over TCP	SNMP trap reception port
1024	SNMP over TCP	SNMP source port
443	RFB over TCP	Remote Keyboard and Mouse data 443

E. Bandwidth Consumption

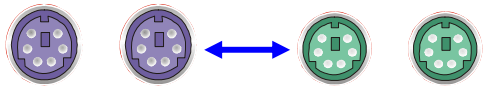
The preconfigured network speed selection simply results in a different Compression and Color Depth configuration in order to match the different bandwidth limitations of the network type (UMTS, ISDN, etc.)

The following suggested network bandwidth planning table for IP-101 installation is from the test results with 3D-Labyrinth screen saver at Resolution 800x600, the worst case consuming the highest network bandwidth.

Compressi	**on**	**Color Depth**	**Used Bandwidth**	**Comment**
Video Optimized	Video Optimized	8 bit	3.0 - 3.3 MB/s	uncompressed, synchronized video data, most bandwidth needed
Video Optimized (high color)	Video Optimized	16 bit	4.3 - 5.0 MB/s	uncompressed, synchronized video data, most bandwidth needed
LAN (high color)	0 (no compression)	16 bit	1.0 - 1.3 MB/s	uncompressed video data
LAN	0 (no compression)	8 bit	500 - 700 kb/s	uncompressed video data
DSL	2	8 bit	110 - 140 kb/s	slower video because of compression
UMTS	4	8 bit	80 - 100 kb/s	slower video because of compression
ISDN 128k	6	4 bit	20 - 30 kb/s	16 colors
ISDN/Modem V.90	7	2 bit	13 - 17 kb/s	gray scale
GPRS/HSCSD	8	2 bit	5 - 7 kb/s	gray scale
GSM Modem	9 (best compression)	1 bit	1 - 3 kb/s	black&white video

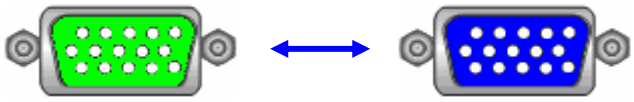
F. Cable Connectors

PS/2 Cable:
Mini Din 6 pin Male to Male



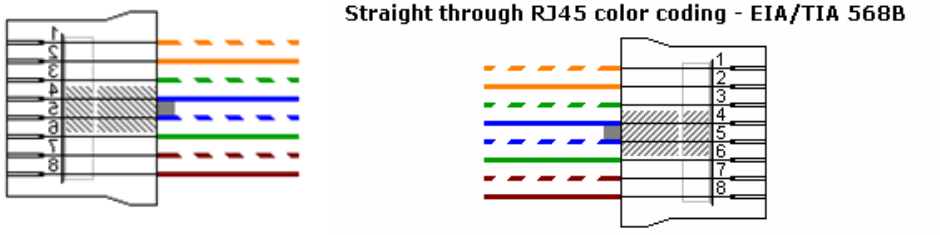
AT to PS/2 keyboard adapter: (Optional)
Din 5 pins Male to Mini Din 6 pin Female

VGA Cable: HD-15 Male to Male



USB 2.0 Cable: USB A-Mini cable

CAT5/5E/6 Straight Through UTP/STP Cable



G. Well-Known TCP/UDP Port Numbers

Port numbers are divided into three ranges: Well Known Ports, Registered Ports, and Dynamic and/or Private Ports. Well Known Ports are those from 0 through 1023. Registered Ports are those from 1024 through 49151. Dynamic and/or Private Ports are those from 49152 through 65535.

Well Known Ports are assigned by IANA, and on most systems, can only be used by system processes or by programs executed by privileged users. Table below shows some of the well-known port numbers. For more details, please visit the IANA website:
http://www.iana.org/assignments/port-numbers

Port Number	Protocol	TCP/UDP
21	FTP (File Transfer Protocol)	TCP
22	SSH (Secure Shell)	TCP
23	Telnet	TCP
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UCP
39	RLP (Resource Location Protocol)	UDP
49	TACACS, TACACS+	UDP
53	DNS	UDP
67	BOOTP server	UDP
68	BOOTP client	UDP
69	TFTP	UDP
70	Gopher	TCP
79	Finger	TCP
80	HTTP	TCP
110	POP3	TCP
119	NNTP (Network News Transfer Protocol)	TCP
161/162	SNMP	UDP
443	HTTPS	TCP

H. Protocol Glossary

BOOTP (Bootstrap Protocol)
Similar to DHCP, but for smaller networks. Automatically assigns the IP address for a specific duration of time.

CHAP (Challenge Handshake Authentication Protocol)
A secure protocol for connecting to a system; it is more secure than the PAP.

DHCP (Dynamic Host Configuration Protocol)
Internet protocol for automating the configuration of computers that use TCP/IP.

DNS (Domain Name Servers): A system that allows a network name server to translate text host names into numeric IP addresses.

Kerberos
A network authentication protocol that provides strong authentication for client/server applications by using secret-key cryptography.

LDAP (Lightweight Directory Access Protocol)
A protocol for accessing directory information.

NAT (Network Address Translation)
An Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. This enables a company to shield internal addresses from the public Internet.

NFS (Network File System)
A protocol that allows file sharing across a network. Users can view, store, and update files on a remote computer. You can use NFS to mount all or a portion of a file system. Users can access the portion mounted with the same privileges as the user's access to each file.

NIS (Network Information System)
System developed by Sun Microsystems for distributing system data such as user and host names among computers on a network.

NMS (Network Management System)
NMS acts as a central server, requesting and receiving SNMP-type information from any computer using SNMP.

NTP (Network Time Protocol)
A protocol used to synchronize time on networked computers and equipment.

PAP (Password Authentication Protocol)
A method of user authentication in which the username and password are transmitted over a network and compared to a table of name-password pairs.

PPP (Point-to-Point Protocol)
A protocol for creating and running IP and other network protocols over a serial link.

RADIUS (Remote Authentication Dial-In User Service)
An authentication and accounting protocol. Enables remote access servers to communicate with a central server to authenticate dial-in users and their access permissions. A company stores user profiles in a central database that all remote servers can share.

SNMP (Simple Network Management Protocol)
A protocol that system administrators use to monitor networks and connected devices and to respond to queries from other network hosts.

SMTP (Simple Mail Transfer Protocol)
TCP/IP protocol for sending email between servers.

SSL (Secure Sockets Layer)
A protocol that provides authentication and encryption services between a web server and a web browser.

SSH (Secure Shell)
A secure transport protocol based on public-key cryptography.

TACACS+ (Terminal Access Controller Access Control System)
A method of authentication used in UNIX networks. It allows a remote access server to communicate with an authentication server to determine whether the user has access to the network.

Telnet
A terminal protocol that provides an easy-to-use method of creating terminal connections to a network host.